FACULDADE CÁSPER LÍBERO

Marina Nossa Neto

A Máquina de ódio da Internet:

As operações do Anonymous como impacto do hacktivismo contemporâneo e a consciência política ativista na Era da Informação

São Paulo

2016

MARINA NOSSA NETO

A Máquina de ódio da Internet:

As operações do Anonymous como impacto do hacktivismo contemporâneo e a consciência política ativista na Era da Informação

Trabalho de conclusão de curso de Pós-graduação lato sensu apresentado à Faculdade Cásper Líbero como requisito parcial para a especialização em Teorias e Práticas em Comunicação

Orientador: Prof. Me. Liráucio Girardi Júnior

SÃO PAULO

2016

MARINA NOSSA NETO

A Máquina de ódio da Internet:

As operações do Anonymous como impacto do hacktivismo contemporâneo e a consciência política ativista na Era da Informação

Trabalho de conclusão de curso de Pós-graduação lato sensu apresentado à Faculdade Cásper Líbero como requisito parcial para a especialização em Teorias e Práticas em Comunicação

Orientador: Prof. Me. Liráucio Girardi Júnior

____

Data da aprovação

Banca Examinadora:

____

Prof. Me. Liráucio Girardi Júnior

Faculdade Cásper Líbero

____

Profa. Me. Dra. Roberta Brandalise

Faculdade Cásper Líbero

São Paulo

2016

Dedico este trabalho a todos os lutadores pela resistência de uma Internet mais livre, transparente e independente. Aos que lutam para concretizar um sistema de distribuição de informação para o espaço virtual, à sociedade e ao cidadão comum. Aos visionários e ativistas de cibersegurança e aos hackers que transformaram a Internet como conhecemos hoje.

AGRADECIMENTOS

Aos meus pais e irmão, pelo incentivo, paciência e compreensão na utilização de grande parte do meu tempo para motivação e esforço durante a produção e conclusão deste trabalho.

Aos meus professores de Pós-graduação da Faculdade Cásper Líbero, em especial, ao orientador Liráucio, pela atenção e incentivo no processo de pesquisa da minha monografia.

Aos usuários da rede OnionIRC e aos membros do Anonymous que aceitaram contribuir e atribuir detalhes para o conteúdo desta monografia: AnonDiscordian, Pr1m1t1v3, butts, The Gangster e KarmaCop.

Eles (Anonymous) são de um tipo de garotos rudes do hacktivismo. Há uma linha tênue de delicadeza e simpatia entre eles, mas também acho que é uma razão pela qual eles conseguem acumular tanto amor e ódio das pessoas. Eles representam um certo tipo de liberdade caótica.

(Gabriella Coleman, 2012).

RESUMO

O coletivo Anonymous foi o principal catalizador de debates sobre ataques de negação de serviço – DDoS – nos últimos anos, como uma tática de protesto legítimo, o que tem estimulado reflexões sobre a credibilidade das operações que partem do princípio da cultura hacker. A diversidade da política dos hackers, em particular o Anonymous, também deriva dos princípios liberais e a ética hacker inclusa na subcultura do hacktivismo. Enquanto o Anonymous ainda não obteve a chance de ocupar um espaço livre de controvérsias no cenário da Internet, em fevereiro de 2012, o coletivo começou a ser retratado como uma marca de protesto radical político e não necessariamente como desordeiros que persistiam em desencadear extremistas e atos caóticos ao interferir servidores e sites. Os ativistas do Anonymous são mais eficazes e contundentes ao lutar contra a censura. Com campanhas como a Operação Payback, que visava empresas como MasterCard quando interromperam serviços de doação ao WikiLeaks, OpTunisia, como resposta à tática do governo tunisiano contra os manifestantes e jornalistas, OpJapan e OpMegaupload, lançada em resposta à legislação de direitos autorais e a mais recente e controversa OpISIS, contra as forças do Estado Islâmico e sua propaganda na Internet.

Palavras-chave: Anonymous. Hacktivismo. Coletivo. Internet. Cultura Hacker.

ABSTRACT

The collective Anonymous was the main catalyst for debates about denial of service attacks - DDoS - in recent years, as a legitimate protest tactic, which has stimulated reflections on the credibility of operations related to the hacker culture. The diversity of political hackers, in particular Anonymous, also derives from the liberal principles and the ethical hacker included in the subculture of hacktivism. While Anonymous didn't have a chance to occupy a space of controversy in the Internet scenario, in February 2012, the group began to be portrayed as a political radical protest brand and not necessarily as troublemakers who persisted in extremist trigger and chaotic acts to interfere world servers and websites. Anonymous activists are more effective and compelling to fight against censorship. With campaigns like Operation Payback, aimed at companies like MasterCard when stopped giving services to WikiLeaks, OpTunisia in response to the tactics of the Tunisian government against demonstrators and journalists, OpJapan and OpMegaupload, launched in response to copyright legislation and more recent and the controversial Operation ISIS, against the forces of the Islamic State and its propaganda on the Internet.

Keywords: Anonymous. Hacktivism. Collective. Internet. Hacker culture.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

O fenômeno da Internet trouxe à sociedade virtual uma nova forma de participação política na Internet, difundindo à comunidade do ciberespaco o sentido da liberdade de expressão e transparencia de informação em diversas formas de comunicação. O hacktivismo irá ajudar a elucidar essa questão. Em particular, as ações orquestradas pelo grupo de ativistas da Internet, o coletivo Anonymous. Para Alexandra Samuel (2004, p.21), enquanto o hacktivismo levanta questões sobre a forma que a liberdade de expressão e o anonimato são alinhados, o movimento também reproduz diversas diretrizes que estimulam cada vez mais a sociedade na singularização entre o ativismo digital e o ciberterrorismo, influenciando futuras formas discursivas de resistência na Internet.

Visto assim, este trabalho irá retratar como o hacktivismo ilustra o desafio de cumprir regras de um prática divergente do ciberterrorismo, na utilização da identidade coletiva com o propósito de criar ações que possam desmitificar o significado de um movimento descentralizado e coordenado por indivíduos que buscam os mesmos objetivos. Para reforçar a importância deste cenário do ativismo digital na conduta do movimento Anonymous, foram apresentados neste trabalho um composto de ideias e hipóteses sobre a influência histórica do coletivo de hacktivistas durante ascensão da cultura da Internet e a forma dos veículos de comunicação em apurar as informações que envolvam o grupo.

O vínculo primordial para a abertura deste estudo é a difusão das comunidades alternativas de ativismo como indícios dos valores da cultura hacker. Sobretudo, esta é a parte onde será contextualizada as operações e os processo de reorganização coletiva durante ataques cibernéticos contra jurisdições governamentais à favor de liberdades civis e transparência de informação na Internet. Em particular, o trabalho será centralizado nas operações do Anonymous, em essencial a *'Operação ISIS'*[1].

[1] Um grupo associado com o movimento Anonymous lançou o que dizia ser uma "guerra total" contra o Estado Islâmico (também conhecido como ISIS ou Daesh), encorajando as pessoas a se juntar em operações supostamente centradas nos perfis das redes sociais associados com a organização terrorista em resposta aos ataques em Paris, em novembro de 2015. Ver em: http://arstechnica.com/tech-policy/2015/11/whos-isis-anonymous-opparis-campaign-against-islamic-state-goes-awry/. Acesso: 12 de Março 2016.

Para Pierre Lévy (2001), a cultura hacker diz respeito ao conjunto de valores e crenças que surgiram das redes de programadores de computador por meio da interação online em torno de sua colaboração de projetos autonomamente definidos de programação criativa. No caso do grupo Anonymous, foi necessária a aglomeração de milhares de usuários no mesmo espaço e tempo para a criação de uma cultura tecnomeritocrática imposta pelo coletivo, que a princípio, desencadeou ações espontâneas para se tornar o cerne da cultura hacker contemporânea (Coleman, 2014).

A literatura utilizada para aprofundar o estudo das perspectivas do hacktivismo na influência das operações do Anonymous é composta por uma grade de múltiplas áreas de estudo, como antropologia, sociologia, filosofia, cibersegurança e ciência da computação. Tanto é que uma das análises deste trabalho irá concentrar o hacktivismo no contexto de desobediência civil e na abrangência midiática sobre as operações do Anonymous.[2] Esta abordagem tem sido mais amplamente realizada no estudo de Pekka Himenam (2004), Tim Jordan e Paul Taylor (1998) e em dissertações da antropóloga Gabriella Coleman (2012).

O primeiro capítulo deste trabalho foi aprofundado no estudo de Steven Levy, Manuel Castells, Parmy Olson e Gabriella Coleman para apresentar o coletivo Anonymous e seu epicentro na comunidade virtual. Em consequência da magnitude das ações de ativismo digital pelo coletivo hacker, os meios de comunicação, exclusivamente os telejornais e a mídia impressa, se utilizam da opinião pública em massa para desestabilizar o discurso do movimento Anonymous ao veicular à mídia as práticas de hacking como meio controverso de ação terrorista ou criminosa, deste modo, enfranquecendo a estigma do ativismo do Anonymous na Internet.

No decorrer do segundo capítulo, será explorada a linha do tempo de operações do ativismo do Anonymous e a incorporação de seus interesses com a Internet na interação de causas políticas, sociais e culturais que visam beneficiar o cidadão comum no ciberespaço. A comunidade hacker é assim, caracterizada por Jordan e Taylor (1998), por um relacionamento sólido com a tecnologia, em particular com técnicas de

---

[2] Dada a natureza disforme do Anonymous - que consiste em um número desconhecido de hackers sem líder ou porta-voz oficial - não surpreende que a chamada à uma ciberguerra resultou em uma reação desproporcional de hackers agindo de forma isolada. Ver em: http://www.cbsnews.com/news/anonymous-vs-isis-social-media-war/ Acesso: 22 de Março 2016.

computação gráfica, códigos, protocolos, princípios básicos da liberdade de expressão na Internet e tecnologia da informação.

O que resultou na abrangência conceitual do hacktivismo, em particular, o coletivo Anonymous, é que esses indivíduos seguem uma lógica própria. A natureza fundamental do movimento é o compromisso com o anonimato e o livre fluxo de informação, sem qualquer apoio político e consistência filosófica. A questão orginária deste trabalho, portanto, é o alicerce das operações dos hacktivistas do Anonymous na manutenção da ideia de uma Internet livre e descentralizada, ao que irá expor o posicionamento duvidoso dos mediadores de comunicação ao enfraquecer o discurso do movimento hacker.

Em meio a conflitos e mudanças quanto ao direcionamento do movimento hacktivista contemporâneo, o terceiro capítulo consiste na inclusão de comentários a partir de entrevistas concedidas por quatro membros do coletivo Anonymous: AnonDiscordian da Holanda, Pr1m1t1v3 e butts, ambos dos Estados Unidos, ex-membro do AntiSec KarmaCop, do Reino Unido. Foi também possível a mediação de uma entrevista, por meio de email, com um porta-voz do grupo de hacktivismo da década de 70, The Cult of the Dead Cow, se autoproclamando como 'The Gangster'.

Em tese, defendo que o coletivo Anonymous merece uma séria atenção como um grupo hacktivista. O coletivo de hackers e visionários da tecnologia tem conquistado atenção considerável da imprensa nos últimos anos, dado que estes hackers são o coletivo disforme mais famoso por publicar constantemente vídeos no YouTube em forma de comunicados de imprensa, identificados com máscaras de Guy Fawkes. Dessa maneira, fica difícil tornar o grupo sério. No entanto, o Anonymous é mais do que apenas um aparelho de "trolling" da Internet e será importante retratar os efeitos das ações desse ativismo digital contemporâneo.

A trajetória do hacktivismo se resume no uso de computadores ou técnicas de hacking para fins políticos e sociais;
o principal instrumento de hacktivismo do Anonymous é a estratégia coletiva sem a mediação de um líder, o que certamente fazem jus à cultura da meritocracia (McLaughlin, 2012). Outra prática comum é o ataque distribuído de negação de serviços (DDoS), uma técnica em que um site é sobrecarregado com o tráfego de acessos e fica offline por tempo inderteminado até que haja uma manutenção interna de servidor.

Desse modo, como Castells afirma (2013), a apropriação de ações diretas pelos hackers, em especial do Anonymous, ilustra um papel fundamental na construção do discurso de uma identidade cultural alternativa na sociedade da informação, o que favorece na disseminação de movimentos de resistência na Internet. Portanto, esses movimentos carregam princípios e diversidades culturais ramificadas do ativismo associado com o hacking.

Parmy Olson (2014) argumenta que o Anonymous emergiu de uma cultura hacker histórica; a retórica do grupo é uma reminiscência da ética hacker, fundada sobre os princípios de acesso livre à informação com preceitos de melhorar a qualidade de vida das pessoas quanto às tecnologias, que se desenvolveu nos anos 80 e 90, juntamente com a ascensão do computador pessoal. Assim como o grupo Anonymous, a ética hacker passou por inúmeras transformações desde seu surgimento.

Há uma série de debates em curso sobre esse coletivo e suas ramificações, por exemplo, sobre o LulzSec e AntiSec, ao nos questionar: suas ações são éticas e positivas? Qual é o resultado das operações de hacking? Qual sua importância? Em '*From the Lulz to Collective Action'*, Gabriella Coleman (2011)[3] cita um membro do grupo: "'Eu vim para o lulz mas fiquei para a ofensa[4]", dizia o Anonymous vestindo uma máscara de Guy Fawkes e protestando contra a Igreja da Cientologia. O Anonymous é assim o símbolo cômico e rebelde da Internet, mas ainda conduzido por uma parte social e política consciente. Logo, este trabalho irá elucidar o que inspirou toda a indignação existente na Internet, tendo em vista as soluções reproduzidas em forma de operações cibernéticas por este coletivo de hackers visionários.

---

[3] Gabriella Coleman em artigo sobre o Anonymous e LulzSec, 06 de Abril de 2011. Ver em: http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action Acesso: 27 de Abril 2016.

[4] Frase popular entre o coletivo Anonymous: "I came for the lulz but stayed for the outrage".

1. A HISTÓRIA DO HACKTIVISMO

A cultura do hacking[5] surge no MIT (Instituto de Tecnologia de Massachusetts), em 1960, onde o termo é cunhado por membros do *Tech Model Railroad Club*[6]. Por 50 anos, o grupo tem se instalado no edifício 20 do campus do instituto, localizado no MIT *Museum Building*. O TMRC utiliza o termo "hacker" apenas em seu sentido original, como "alguém que se aplica uma capacidade de invenção para criar um resultado inteligente" (Levy, 2012).

Jordan e Taylor (1998) afirmam que a comunidade hacker compartilha de uma apreciação minunciosa com a tecnologia e princípios inerentes às liberdades civis na Internet. Essa ótica nos permite compreender que o hacking é baseado no relacionamento mútuo entre tecnologia e indivíduo, na base de ações coletivamente orquestradas, considerando o valor da identidade no processo de uma norma social peculiar no hacktivismo. Por outro lado, Castells (2013) se manifesta quanto à maneira de como a comunidade hacker é projetada, na prática:

> Começa-se a ser um hacker a partir do ímpeto individual de criar, independentemente do cenário institucional dessa criação. É por isso que há hackers na academia, em escolas secundárias, em grandes empresas e nas margens da sociedade. Eles não dependem de instituições para sua existência intelectual, mas dependem, efetivamente, de sua comunidade autodefinida, construída em torno de rede de computadores. Há na cultura hacker um sentimento comunitário, baseado na integração ativa a uma comunidade, que se estrutura em torno de costumes e princípios de organização social informal (Castells, 2013, p. 43).

Na perspectiva histórica, o hacktivismo surge no final de 1980, em um panorama cultural visto como uma ameaça perceptível e conveniente para um período de

---

[5] A cultura do hacking é a ação de encontrar pequenas coisas que possam ser alteradas e modificadas, visando uma mudança iterativa, como os *blueprints* de engenharia que desenvolvedores de software criam. Fundamentalmente, é uma subcultura aliada à ação intencional para afetar uma mudança cultural positiva dentro de sua organização ou comunidade. Ver em: http://www.catb.org/jargon/html/introduction.html. Acesso: 21 de Março 2016

[6] Os hackers do *The Tech Model Railroad Club* adotaram o sistema de ferreomodelismo como seu hobbie tecnológico favorito e inventaram ferramentas de programação, gírias e toda uma cultura em torno do que conhecemos sobre a cultura hacker hoje. Os primeiros anos foram examinados na primeira parte do livro de Steven Levy, "Os Heróis da Revolução", 2012. O TMTC tornou-se o núcleo do Laboratório de Inteligência Artificial do MIT, principal centro mundial de pesquisa de AI durante o início de 1980. Sua influência se espalhou a partir de 1969, o ano do surgimento da ARPANET.

transformaçoes tecnológicas constantes. Um bom exemplo de hacktivismo precoce foi o episódio '*Worms Against Nuclear Killer*' (WANK), um vírus de computador que hacktivistas conseguiram instalar na rede da NASA (Administração Nacional da Aeronáutica e Espaço) e do Departamento de Energia dos Estados Unidos em outubro de 1989, para protestar contra o lançamento de um *air-bus* que carregava plutônio radioativo a Júpiter.[7]

Em 1996, um pequeno grupo de hacktivistas atacavam sites governamentais, substituindo suas *home pages* com mensagens de protesto. Em uma das primeiras invasões, um hacker mudou a página inicial do site do Departamento de Justiça dos Estados Unidos, exibindo imagens sórdidas em protesto contra o *Communications Decency Act* (que mais tarde foi considerado inconstitucional).[8] Assim, o termo "hacktivismo" foi cunhado no mesmo ano pelo *Cult of the Dead Cow* (CDC), uma organização que também deu à luz ao '*Hacktivismo*'[9], um grupo internacional de hackers e ativistas dedicados à luta pelos direitos humanos. Ao invés de lançar ciberataques, o grupo CDC tem utilizado suas habilidades de programação para desenvolver ferramentas de software e apoiar a liberdade de expressão e privacidade na Internet. Estes entusiastas cibernéticos criticam assiduamente o uso de ataques DDoS e desfigurações de interface como uma antítese da liberdade de expressão.

> Através da tecnologia, os hackers denunciam a própria racionalidade tecnológica e o poder constituído por grandes empresas e instituições governamentais. Os hackers são considerados, ainda hoje, os magos da comunidade digital tentando, de todas as maneiras, desvendar mistérios digitais, códigos secretos, desbravar novos espaços virtuais. Eles conhecem muito bem o funcionamento dos sistemas e nem sempre seguem as regras (Lemos, 2013, p. 210).

---

[7] A NASA gastou cerca de meio milhão de dólares em tempo e recursos para fazer a limpeza completa do seu sistema. Até hoje, não se sabe de onde o ataque se originou, embora tenha sido apontado hackers (e crackers) de Melbourne, na Austrália.

[8] O Ato de Decência nas Comunicações (CDA), também conhecido por alguns legisladores como o "*Great Internet Sex Panic of 1995*", foi a primeira tentativa pelo Congresso dos Estados Unidos para regular material pornográfico na web. Em 1997, no caso da lei do marco cibernético de Reno v. ACLU, o Supremo Tribunal dos Estados Unidos revogou as disposições de anti-indecência da lei. Ver em: https://www.eff.org/pt-br/issues/cda230 . Acesso: 21 de Março 2016.

[9] Considerada uma ramificação do CDC (Cult of The Dead Cow), o 'Hacktivismo' se baseia nas crenças do grupo ligadas à *Declaração de Hacktivismo*, que procura aplicar a Declaração Universal dos Direitos Humanos e no Pacto Internacional sobre os Direitos Civis e Políticos na Internet.

Assim como Lemos (2003) descreve a sensatez tecnológica do hacktivismo, Alexandra Samuel (2014) identifica a comunidade hacker como uma constelação cibernética ao direcionar ações de hacking como projetos colaborativos, para que a comunidade de hackers possam implementar uma evasão política na Internet. Segundo Christina Grammatikopoulou (2014), o hacktivismo se enraizou em diferentes culturas que emergiram durante a ascensão das tecnologias de informação, e hoje, estabelecem um paralelo com bens culturais da comunidade virtual com o espaço urbano, seja para fins políticos, culturais, sociais ou econômicos.

> Essa perspectiva de estudo dos hackers tem adquirido relevância não somente porque sua cultura está na origem da Internet, mas devido à importância do chamado Floss (free libre open source software) para a expansão das redes digitais. Trata-se de comunidades de hackers que desenvolvem programas de computador com o códigofonte aberto e com licenças de propriedade permissivas que permitem usar, copiar, estudar completamente, melhorar e distribuir as mudanças realizadas no software (Silveira, 2010, p. 35).

A mídia adotou o termo "hacktivismo" durante o conflito de Kosovo em 1998 e 1999[10], quando ativistas lançaram ataques de DDoS simultâneos, desconfigurando interfaces de sites para protestar contra a guerra e os países envolvidos, o que eventualmente, firmou-se definitivo uma visão contraditória sobre a atividade do hacktivismo: o ciberterrorismo. O grupo de hackers '*Team Spl0it'*, localizado nos Estados Unidos, escreveu "*stop the war*" ao tirar o site da Administração da Aviação Federal[11] fora do ar; o *Russian Hackers Union* deixou o recado "s*top terrorist aggression against Jugoslavia*" no site da Marinha dos EUA; e o grupo Black Hand realizou ataques DDoS contra computadores da Organização do Tratado do Atlântico Norte (OTAN) e outras entidades. Até mesmo hacktivistas chineses se envolveram nas

[10]O conflito começou durante 1998 entre a Iugoslávia e as forças civis, militares e separatistas albaneses em Kosovo. Durante 1999, a OTAN (Organização do Tratado do Atlântico Norte) lançou uma campanha de bombardeio contra a Iugoslávia, com duração de 78 dias. Uma parte da população sérvia sentiu-se no dever de ajudar o país a se defender de alguma ou interromper as operações da OTAN. Entre essas pessoas eram também entusiastas envolvidos no mundo da computação. Ao começar a se organizarem em pequenos grupos, melhor que puderam fazer foi a tentativa de desconfigurar sites e interromper as operações de guerra. Um famoso grupo de hackers que executou maioria dos ataques foram os ativistas do *Black Hand*. Ver em: http://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/. Acesso: 18 de Março 2016.

[11] *Federal Aviation Administration*, da sigla em inglês FAA.

operações de hacking ao desconfigurar sites dos EUA e participando de lançamento de ataques de DDoS mais intensos após o bombardeio da embaixada chinesa em Belgrado, na Iugoslávia.

Na virada do século 20, o hacktivismo havia se tornado um meio trivial de protesto, coexistindo entre conflitos militares e internacionais, bem como protestos de rua. A empresa de inteligência *iDefense* tem informado em nota que durante os primeiros meses da Segunda Intifada Palestina, que eclodiu entre Israel e os palestinos em setembro de 2000, mais de 30 pró-palestina, 10 grupos de hacktivismo pró-Israel e hacktivistas inciaram uma guerra cibernética. Mais tarde, os ataques terroristas de setembro de 2001, provocados pela Al-Qaeda e o início da *Operation Enduring Freedom*[12] deram a luz à grupos como o *Young Intelligent Hackers Against Terrorism*[13], que teve como objetivo interromper o financiamento de terroristas e uma coalizão de grupos de hackers paquistaneses chamados de *Al-Qaeda Alliance online*.

Apesar de sua prevalência durante mais de duas décadas, o hacktivismo vem sendo frequentemente associado com as ações do grupo Anonymous, o coletivo descentralizado de ativistas e hackers conhecido pela personificação simbólica com máscaras de Guy Fawkes[14] e o uso da imagem de um indivíduo vestindo terno com um ponto de interrogação no lugar da cabeça. De acordo com Gabriella Coleman (2012), há também outras maneiras diferentes apoiadas pelo coletivo Anonymous para defender a internet, como por exemplo, desenvolver diferentes tipos de softwares de código aberto ou se associar ao Partido Pirata[15]. Este é o hacktivismo contemporâneo originado da camada rebelde do espaço virtual.

---

[12] A Operação Liberdade Duradoura (em inglês: *Operation Enduring Freedom - OEF)* foi a resposta militar do governo dos Estados Unidos aos Ataques de 11 de Setembro de 2001.

[13] O fundador da YIHAT (sigla do grupo hacker), Schmitz, é um ex-hacker de 27 anos que virou magnata *high-tech*, na Alemanha. Segundo o hacker, o grupo começou a partir da demanda de dezenas de ligações de cidadãos de todo o mundo sobre seu anúncio de uma recompensa de US $ 10 milhões por informações que levem à captura de Osama bin Laden, após os ataques de 11 de Setembro. Ver em: http://abcnews.go.com/Technology/story?id=98236&page=1. Acesso: 06 de Abril 2016.

[14] A utilização da máscara de Fawkes e o fato de Guy Fawkes ter explodido o parlamento britânico, foi considerada uma simbologia de re-apropriação e representação política vista no filme 'V de Vingança', de 2006. A crença do movimento Anonymous, assim, ao usar a máscara de Guy Fawkes, simboliza um desejo verdadeiramente democrático de mudança e revolução.

[15] O Partido Pirata Internacional (PPI) é uma organização sem fins lucrativos não governamental internacional com sede em Bruxelas, Bélgica. Formada em 2010, o PPI serve como uma organização mundial para o defensores de direitos humanos na Internet, representando membros de 41 países. O PPI é formado por movimentos políticos da liberdade de expressão, tentando alcançar os seus objetivos pelos meios do sistema político estabelecido utilizando-se também do ativismo. Ver em: http://www.pp-international.net/about. Acesso: 2 de Abril 2016.

> Anonymous in its 'original form' is dead. There are still pockets of Anons that hang onto the old ways but a lot of the newer Anons have 0 clues what it's about. Many are hell bent on being SJWs and forget about the lulz. There seems to be a growing amount of infighting and personal agendas that make it difficult, if not impossible, to get any real, new Ops started with the Hive at large. Small teams are where it should be now[16].

O Anonymous é uma parte distinta da comunidade virtual, que emergiu de um cenário político diverso e crítico. O movimento, portanto, fornece uma rara contramedida em atos, palavras e símbolos contra uma sociedade que incentiva os cidadãos a revelarem suas vidas, no espaço em que a Internet armazena informações sobre os usuários e bancos de dados do governo – e a um momento em que a capacidade das autoridades de vigiar as fronteiras digitais dos usuários tem crescido exponencialmente graças ao baixo custo das tecnologias digitais onipresentes e às novas parcerias público-privadas de movimentos sociais na Internet (Coleman, 2014).

Em 2003, aos 15 anos, Christopher Poole fundou o webblog 4chan.org, de seu quarto em Nova Iorque, o que culminou a ascensão de uma subcultura necessária para a Internet. O site acumula atenção principalmente por sua proliferação de memes humorísticos de gatos – que foi cunhado o termo pela cultura hacker como ‘lolcats’ - e momentos de ‘trollagem’ e ícones de memes eternizados pela cultura hacker, como o “Rickroll”, referindo-se ao hit dos anos 80 de Rick Astley, "Never Gonna Give You Up". (Coleman, 2012).

Mas com o tempo, Pool conseguiu atrair um exército mundial de hackers anônimos, muitos deles politizados, que recriaram um hábito de compartilhamento de informações de forma colaborativa, incluindo ferramentas de hacking e, eventualmente, efetivação de ciberoperações. O que começou como uma série de brincadeiras realizadas por diversão ociosa, evoluiu gradualmente em uma aglomeração coletiva, compartilhando das mesmas ideias de desobediência civil e combate à corrupção pelo mundo.

---

[16] Tradução nossa: O Anonymous, em sua forma original, está morto. Ainda há poucos Anons que se apegam aos bons e velhos tempos, mas uma grande parte da nova geração de Anons têm 0 ideia do que se trata. Muitos estão bastante concentrados em se tornar um tipo de SJWs (social justice warriors) e esquecer do ‘lulz’. Parece que há uma quantidade crescente de lutas e agendas pessoais que tornam difícil, se não impossível, para obter quaisquer reais, novas Ops que começaram com o grupo em geral. Os pequenos grupos estão onde deveriam estar agora. Resposta do ‘Anon’ Pr1m1t1v3, em 13 de Abril de 2016, por e-mail.

1.2 A GUERRILHA DO ANONYMOUS

Enquanto o *Electronic Disturbance Theater* [17]e outros grupos se basearam em filosofias políticas e um ideal cultural dentro no panorama anti-capitalista da cultura ativista, as ações do coletivo Anonymous são fortemente incorporadas dentro do restrito, em um cenário cultural limitado (Sauter, 2013).

O Anonymous surgiu em 2003, mas não em grande escala até 2008 quando o grupo lançou o “Projeto Chanology”, episódio em que o ator norte-americano Tom Cruise, ao se tornar defensor da Igreja da Cientologia, participou de uma entrevista em 2004 com documentaristas da própria Igreja, tornando o vídeo um conteúdo publicitário. Porém, a imagem da instituição se mostrou ameaçada após o ator expor declarações que não estavam de acordo com as ideias da Cientologia[18], ou seja, não disponibilizaram a entrevista até 2007, quando um membro anônimo da Igreja decidiu tornar o conteúdo público no YouTube, viralizando-se pela rede e até mesmo no fórum do 4Chan[19]. No fórum do 4Chan, a onda de usuários se manifestando contra as ações da Cientologia cresceu em nível inesperado. A partir desse ponto, se criou no ‘/b/’[20] um manifesto para que a comunidade virtual aja de maneira vertiginosa, com o título “Ataque à Cientologia”:

> Acho que é hora de o /b/ fazer algo importante. As pessoas têm de entender que ninguém mexe com o /b/...Estou falando em “hackear” ou “derrubar” o site oficial da Cientologia. É hora de

[17] Fundada em 1997 pelo artista e escritor Ricardo Dominguez, EDT é uma companhia digital de ativistas cibernéticos, acadêmicos e artistas performáticos da comunidade virtual que se empenham no desenvolvimento da teoria e prática de atos não-violentos através do espaço digital e urbano. Como um grupo coletivo desenvolveram um software de computador para exibir suas ideias contra as ações militares anti-propagandista e, consequentemente, mobilizando usuários a agir em solidariedade à causa, dando início à presença coletiva em ações diretas na Internet. Ver em: http://www.digicult.it/hacktivism/no-borders-struggles-the-electronic-disturbance-theatre-2-0/ . Acesso em 03 de Abril 2016.

[18] Entrevista com Tom Cruise sobre a Cientologia: https://www.youtube.com/watch?v=UFBZ_uAbxS0. Acesso em 03 de Abril 2016.

[19] A Igreja não estava exatamente interessada em que o vídeo vazasse. O ex-cientologista, Pieniadz arquivou o vídeo por quase um ano, esperando uma ocasião apropriada para revelá-lo, no momento em que Tom Cruise teria sua biografia lançada, em 15 de janeiro de 2008. A Igreja da Cientologia era conhecida por processos litigiosos. Entre os principais objetivos da entidade está o surgimento de uma civilização sem insanidade, criminosos e guerra, na qual o homem prosperaria e seria livre para se elevar em sua verdadeira natureza espiritual, deixando de lado a imagem de igreja convencional.

[20] Também conhecido “random”, o /b/ foi o primeiro fórum do site, e a área que mais recebe tráfego. Como o próprio nome sugere, era considerado como a fábrica de memes da Internet e o epicentro de “trolling” e grande acesso de usuários em anonimato.

> utilizar nossos recursos para fazer algo em que acreditamos. É hora de fazer algo importante de novo, /b/. Conversem uns com os outros, encontrem um melhor lugar para planejar o ataque e então executem o que pode e deve ser feito. Chegou a hora, /b/.[21]

Desde então, o Anonymous, juntamente com suas ramificações através da comunidade virtual, tem sido responsável por milhares de ataques cibernéticos em todo o mundo, incluindo a amplificação da luta por liberdade de expressão e transparência na Internet. Para Sauter (2013), o Anonymous é representado por um aspecto profundamente performativo. O coletivo se baseia na aglomeração de hackers para a aplicação ferramentas de tecnologia, softwares de código aberto, bem como visto na emancipação da cultura da internet - memes e trolling -, empenhando-se na criação de estereótipos de identidade pública como símbolo anárquico da Internet - ou os *cyberpunks* -, em uma conduta bem-humorada, alimentando reações de medo ou raiva em uma camada desinformada da sociedade.

> Nesta área, o empenho dos hackers tem sido principalmente o de empregar técnicas de engenharia reversa para obter acesso às informações protegidas pelos formatos em quetão. È dessa forma, por exemplo, que documentos utilizados no mundo – o Office, da Microsoft – podem ser acessados por pacotes que se valem unicamente de softwares livres, como é o caso do LibreOffice. Vários embates já foram travados no campo dos formatos e, invariavelmente, os hackers são atores mais que relevantes nessas disputas (Machado, 2013, p. 44).

O ativismo adotado por estes hackers é, no entanto, relativamente fácil de se conduzir, levando em conta o baixo custo e sem necessidade de locomoção física. Indivíduos com pouca ou nenhuma habilidade técnica podem utilizar softwares gratuitos e de fácil acesso, tal como o LOIC ou *Low Orbit Ion Cannon*[22], o qual permite lançar ataques de DDoS (Coleman, 2012). Por outro lado, a maioria dos ciberataques realizados por hacktivistas são ilegais sob estatuto de crimes domésticos. Alguns casos,

---

[21] Trecho do fórum “Ataque à Cientologia”, publicado no 4chan. OLSON, Parmy; p.72, 2014.

[22] LOIC é um software desenvolvido por usuários e/ou hackers do 4Chan destinados a - quando usado en massa por milhares de anônimos - lançamento de *Distributed Denial of Service* (DDoS) para ataques a websites, como ocorrido com a Operação PayPal, em suporte ao WikiLeaks, direcionando acessos múltiplos por segundo, nos sites da Visa, Mastercard e Amazon. O LOIC basicamente transforma a conexão de rede do computador em um catalizador de erros internos de acesso do servidor. Ver em http://gizmodo.com/5709630/what-is-loic. Acesso em 09 de Abril 2016.

no entanto, chegam ao ponto de sofrer acusação judicial, em parte, pois as penalidades são geralmente mínimas. Porém, a desconfiguração de websites são facilmente restaurados, e ataques de negação de serviço - comumente visto na sigla DdoS – que muitas vezes têm pouco ou nenhum impacto.[23]

Mesmo que comunidades ativistas como o Anonymous consigam reivindicar o crédito por suas ações, esses magos da Internet não revelam suas identidades por trás dos codinomes. A menos que os danos sejam significativos, suas ações podem ser susceptíveis de investigação por entidades governamentais. Ainda assim, uma das ramificações do coletivo Anonymous, o LulzSec, seus membros foram identificados e julgados por violar leis cibernéticas.

> Before the arrests occurred, Anonymous wasn't what it was originally intended to be. Everyone used pseudonyms by which they could be recognized. These handles used specific language, were active during specific timezones and had their specific preferences in what they enjoyed, they were identifiable if you met them offline. sup_g (aka Jeremy Hammond) was even handing out proof of his hacking days in LulzSec at Occupy Chicago. There was a lack of understanding anonymity as they would think a VPN would suffice to hide their identities. The FBI knew this was the case, and that the members would be arrested anyway. It was a bonus that they could use a trusted #antisec member to cause distrust within the movement.[24]

Visto assim, Coleman (2012) afirma que além de um compromisso fundamental com o anonimato e o livre fluxo de informações, o Anonymous tem dedicado cada vez mais suas energias para uma dissidência digital e nas ações diretas em torno de operações, sem contar com uma trajetória definitiva. Desta maneira, o Anonymous ainda é um movimento determinado na vontade coletiva para um mal necessário da

[23] Trecho citado na conferência “Beyond HOPE” pelo grupo de hackers underground *Cult of the Dead Cow*, em agosto de 1997, Nova Iorque. Ver em: https://www.youtube.com/watch?v=tUoEo1tViTY Acesso em: 11 de Abril 2016.

[24] Tradução nossa: Antes das prisões ocorrerem, o Anonymous não era o que foi originalmente destinado a ser. Todos usavam pseudônimos pelos quais poderiam ser reconhecidos. Esses codinomes eram de uma linguagem específica, estavam ativos durante fusos horários específicos e tiveram suas preferências específicas no que eles gostavam, eram identificáveis se encontrássemos com eles offline. sup_g (conhecido como Jeremy Hammond) entregou a prova de todo o hacking que havia cometido no LulzSec durante o ‘Occupy Chicago’. Houve uma falta de compreensão sobre anonimato em como eles iriam esconder suas identidades utilizando apenas um software de VPN. O FBI sabia que este era o caso, e que os membros seriam presos de qualquer maneira. Foi um bônus usar um membro confiável do #antisec para causar desconfiança dentro do movimento. Pastebin publicado pelo membro AnonDiscordian em seu perfil no Twitter, sobre a história do Anonymous na sua perspectiva http://pastebin.com/33SQXBu3. Acesso: 27 de Março 2016.

comunidade virtual, sendo que ainda estão intimamente ligados à cultura estridente dos sites de imageboard, ao que tudo indica que o coletivo continuará a espalhar seus rastros da cultura hacker nas múltiplas camadas do ciberespaço.

A relevância do movimento e da ideia intríseca estruturada, porém, ainda permeiam nas subdivisões de grupos de ativismo virtual. O Anonymous age de forma, que às vezes, é vista como irrelevante, ocasionalmente destrutiva, vingativa, e, geralmente, são desdenhosos à lei mas que também conseguem oferecer uma lição moral. (Coleman, 2012, p. 86). Por outro lado, as atividades do Anonymous, díspares e paradoxais em sua superfície, têm sido aproveitadas diante de um profundo desencanto com o status quo político, sem se apoiar em uma visão utópica na agenda global da Internet.

> Activities under the Anonymous banner, such as those of Lulzsec, show that even though Anonymous has gained a measure of respect because it champions free speech and privacy causes, it is also notorious for its irreverent and controversial approach to dissent. To be sure, most of its activities are legal, but a small subset of tactics – such as DDoS attacks and hacking – are illegal, a criminal offence under all circumstances. These tactics also score the most headlines. Some, like 'doxxing' (the leaking of personal, sensitive information, such as social security numbers and home addresses), reside in a 'legal grey zone' because mined information is found on publicly accessible websites (Coleman, 2012, p. 66).[25]

Portanto, até aqui, o grupo Anonymous conseguiu aprimorar uma estutrura de ativismo virtual por meio de recursos técnicos como o *Internet Relay Chat* (IRC)[26], que é executado e administrado por um conjunto de usuários que utilizam do espaço

---

[25] Tradução nossa: As atividades sob a bandeira do Anonymous tais como aquelas do Lulzsec, mostram que embora o Anonymous tenha ganho certo respeito por defender as causas de liberdade de expressão e privacidade, também é notório por sua abordagem irreverente e controversa dissidência. Para ter certeza, a maior parte das suas atividades são legais, mas um pequeno subconjunto de táticas - como ataques de DDoS e hacking - são ilegais, uma ofensa criminal em todas as circunstâncias. Estas táticas também ganham mais manchetes. Algumas, como o 'doxxing' (vazamento de informações pessoais, confidenciais, como contas de redes sociais e endereços residenciais), são vistos em uma 'zona cinzenta legal', porque a informação extraída é encontrada em sites de acesso público.

[26] Desenvolvido em agosto de 1988, por Jarkko Oikarinen, IRC é a abreviação de Internet Relay Chat, um serviço popular de chat em uso até hoje. O IRC permite aos usuários se conectarem a um servidor usando um programa de software ou serviço de Internet para se comunicar uns com os outros, instantaneamente. Para se conectar e conversar com outros usuários do IRC, é necessário um servidor de IRC ou uma interface de web projetada para recepção de várias conexões simultâneas. Ver em: http://www.computerhope.com/jargon/i/irc.htm. Acesso: 12 de Abril 2016.

descentralizado para a orientação de indivíduos interessados em um movimento ativista ou objetivos isolados, os quais têm participado de processos de triagem a partir de normas éticas próprias que tendem a ser estabelecidas consensualmente e executadas por todos os membros da comunidade.

Entre vários acontecimentos, entre 2010 e 2013, que envolveram atividades de hacking, trollagem e *web defacement*[27] em sites de grandes corporações, a presença da NSA (Agência Nacional de Segurança) em fatos jornalísticos sobre a ameaça aos ativistas do Anonymous, na verdade, não conseguiu impulsionar na consciência do público. Entretanto, é possível uma comoção pública se a NSA tivesse, por exemplo, canalizado toda sua atenção entre Maio e Julho de 2011, no auge dos ataques liderados pelo LulzSec.

Em contraste com a maioria das ações do Anonymous, o LulzSec, um grupo de hackers divergente de qualquer outro, agiu de maneira excêntrica, com suas práticas de hacking nem sempre vinculadas à questões políticas. O Lulzsec, por vezes tirava sites do ar para dar declarações morais e políticas e, em outros casos, por brincadeiras - ou "for the lulz"[28]. Durante este período, a atenção da mídia foi focada no Anonymous como apenas adolescentes hackers imprudentes sem causa e não como um grupo de indivíduos que visam lutar por uma Internet livre.

1.3 O EFEITO LULZEC

No início de Maio de 2011, o site da Fox foi o princípio de uma nova retaliação hacktivista, como alvo de um novo grupo de hackers que havia se formado em chatrooms confidenciais promovidos pelo Anonymous. O LulzSec – hackers renegados, que romperam momentaneamente com o Anonymous - surgiram alguns meses após o episódio contra a HBGary Federal[29]. A partir daí, os hackers decidiram atentar-se a

[27] Desconfiguração de interface de um website.

[28] "*Lulz*" é normalmente usado como "I did it for the lulz" ou 'IDIFTL', com a junção do LOL (Laughing Out Loud) e o 'Z' incorporado nas situações que envolvam o 'trolling' ou 'Internet drama' descrito por usuários do 4Chan e na comunicação da cultura hacker. Ver em: https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail. Acesso em: 14 de Abril 2016.

[29] É uma empresa subsidiária da *ManTech International*, focada em segurança de tecnologia. No passado, prestava serviço para duas empresas distintas, vendendo seus produtos para o Governo Federal dos

alvos de diferentes graus em operações simultâneas: a emissora norte-americana PBS, empresas de video games como a Nintendo, Bethesda Studios e a Sony Network, sendo que essa última, os hackers invadiram e expuseram publicamente 24,6 milhões de dados privados de usuários, consequentemente fazendo com que a empresa desativasse o servidor por alguns dias. O LulzSec se autoproclamaram como os "piratas dos últimos dias". De acordo com membros do LulzSec, suas atividades de hacking não tinham propósito definido, mas era simplesmente pelo lulz - a pura vontade de conduzir um caos recreativo na Internet.

Diferente de qualquer relacionamento na cultura hacker convencional, os membros do LulzSec sabiam da identidade de cada um: Ryan Cleary, de Wickford, Essex, foi "Viral"; Jake Davis, de Lerwick, Ilhas Shetland, tinha o nickname "Topiary"; Mustafa Al-Bassam, do sul de Londres, foi "Tflow"; Ryan Ackroyd, em Mexborough, South Yorkshire, era "Kayla", um ex-recruta do exército norte-americano, adotando um codinome feminino, a fim de enganar aqueles que tentavam descobrir a sua identidade real. Seu líder ostensivo "Sabu", de Nova Iorque, era Hector Xavier Monsegur, um porto-riquenho programador nato.

Na leitura de Parmy Olson (2014), a principal ideia dessa subdivisão de hackers, era fazer o que fosse necessário para inspirar o Anonymous como novo ‘lulz’ e, talvez, atrair os holofotes novamente. Por isso, os membros decidiram com unanimidade que não queriam ser limitados por amplos princípios subjacentes ao Anonymous, que eram: em primeiro lugar, a escolha de alvos vistos como opressores da liberdade de expressão; em segundo, não atacar a mídia.

> Nem todos os hackers tinham a simpatia em relação ao Anonymous. Suas intervenções eram muitas vezes demasiadas e tecnicamente sofisticadas para se ter um respeito na comunidade. Alguns hackers sentiam que suas táticas danificaram a maior causa da liberdade na Internet, enquanto uma minoria via suas ações como triviais. E, para outros hackers este era sim um estilo geral de um ativismo perturbador, porém interessante, que simplesmente não era o que fariam. Mas com o LulzSec, era uma história diferente. Um número surpreendente de hackers, especialmente hackers de segurança, adoravam o novo grupo, ou pelo menos estabeleciam uma relação ambivalente (Coleman, 2014, p. 256).

Estados Unidos. Seus outros clientes incluíam firmas especializadas em TI, seguros, emergências informáticas e de coleta de dados. Ver em: http://www.computerworld.com/article/2470536/cybercrime-hacking/hbgary-federal-quits-rsa-over-anonymous-wikileaks-email.html. Acesso em: 12 de Abril 2016.

Depois de 50 dias de lulz , o LulzSec havia chegado ao seu fim. Em 3 de junho, quando desconfiguram o site do FBI, dois membros deixam o grupo preocupados com uma retaliação judicial. Um registro do chatroom, obtido pelo jornal britânico The Guardian[30] nesse período, mostram que Hector Monsegur, como "Sabu", disse ao resto do grupo: "Vocês perceberam que o FBI pôde rastrear o nosso canal, e isso significa que todos aqui devem reforçar sua segurança." Em seguida, no dia 7 de Junho de 2011, Monsegur, que geralmente tinha o hábito de navegar na Internet com o sistema do Tor, havia esquecido de utilizar a ferramenta quando realizava o login em um fórum de bate-papo do Anonymous.

Em consequência disso, após uma sequência de esforços, entre investigações e infiltrações nos canais de comunicação estruturados pelo movimento de hacktivistas, o FBI rastreou Sabu assim quando voltava para sua casa, em Manhattan. Logo depois, os agentes apareceram em sua porta com uma oferta: ser preso ou cooperar com uma operação. Monsegur, que havia assumido o cuidado parental de suas duas sobrinhas, não aceitava o fato de que elas poderiam ser enviadas para um orfanato caso escolhesse a prisão; Sabu optou pela segunda opção. Logo, sem dúvida, o caminho de Monsegur decidiu o destino do LulzSec.

Para concluir o fim do LulzSec, o grupo lançou juntamente ao release final[31], um compilado de documentos hackeados: informações de login de usuários a partir de uma variedade de fontes, incluindo da AOL (provedor de serviços de Internet - America Online) e AT&T (companhia americana de telecomunicações - American Telephone and Telegraph).

> We are Lulz Security, and this is our final release, as today marks something meaningful to us. 50 days ago, we set sail with our humble ship on an uneasy and brutal ocean: the Internet. The hate machine, the love machine, the machine powered by many machines. We are all part of it, helping it grow, and helping it grow on us. For the past 50 days we've been disrupting and exposing corporations, governments, often the general population itself, and quite possibly everything in between, just because we could. All to selflessly entertain

---

[30] Registros de conversas do fim das atividades do LulzSec, exibem o desmembramento do grupo após implicações pessoais. Ver em https://www.theguardian.com/technology/2011/jun/24/inside-lulzsec-chatroom-logs-hackers. Acesso: 11 de Abril 2016.

[31] O último release do LulzSec após 50 dias de atividade. Ver em http://pastebin.com/1znEGmHa. Acesso: 23 de Abril 2016.

> others - vanity, fame, recognition, all of these things are shadowed by our desire for that which we all love. The raw, uninterrupted, chaotic thrill of entertainment and anarchy. It's what we all crave, even the seemingly lifeless politicians and emotionless, middle-aged self-titled failures. You are not failures. You have not blown away. You can get what you want and you are worth having it, believe in yourself. (…). Let it flow...Lulz Security - our crew of six wishes you a happy 2011, and a shout-out to all of our battlefleet members and supporters across the globe.[32]

Como toda comunidade digital tem o efeito de se expandir em diretrizes na camada da Internet, o grupo LulzSec levantou novos paradigmas do cenário do hacktivismo atual, o que possibilitou a inclusão de uma nova onda de entusiastas e aspiradores de ferramentas de tecnologia para contribuir no ativismo digital que havia se erguido mais uma vez.

Em *"Our Weirdness is Free"*, Coleman (2012) relaciona a influência do LulzSec na cultura hacker como um exemplo enaltecido por ramificações singulares da cultura hacker, sobretudo pelo fato de que a figura de Sabu tornou-se uma celebridade para quem estivesse conectado às ações da cena do hacktivismo na época. O condutor do '*lulz*', assim assinalado por Gabriella Coleman (2014), ilustrou a diferença real entre o LulzSec e o Anonymous: o primeiro, priorizou por 50 dias, uma manada de atividades aleatórias na utilização da capacidade insubestimável de hackear com o objetivo de identificar vulnerabilidades de segurança para grandes corporações. Do outro lado, o Anonymous é visto como uma ideia descentralizada, pertinente às causas políticas, sociais e no que diz respeito à liberdade de expressão e transparência na Internet, e consequentemente, na sociedade. A impossibilidade de formar uma imagem abrangente

[32] Tradução nossa: Nós somos o Lulz Security e esta é o nosso último release, como hoje marca algo significativo para nós. 50 dias atrás, partimos com o nosso humilde navio em um oceano inquieto e brutal: a Internet. A máquina de ódio, a máquina de amor, a máquina alimentada por muitas máquinas. Somos todos parte dela, ajudando a crescer, e ajudando-a crescer em nós. Nos últimos 50 dias estivemos perturbando e expondo corporações, governos, muitas vezes, a própria população em geral, e muito possivelmente todos juntos, porque nós podemos. Tudo para entreter altruísticamente outros - vaidade, fama, reconhecimento, todas essas coisas são sombreadas por nosso desejo do que todos nós amamos. A matéria, ininterrupta emoção, caótico de entretenimento e anarquia. É o que todos anseiam, mesmo os políticos que aparentemente inertes e sem emoções, fracassados de meia-idade. Vocês não são falhas. Você não causaram nenhum desastre. Vocês podem ter o que quiserem e vale a pena acreditar em si mesmo. (...). Deixe fluir ... LulzSecurity - a nossa tripulação de seis, desejamos a todos vocês um feliz 2011, e uma mensagem de saída para todos os nossos membros do front de batalhas e apoiadores em todo o mundo.

e consistente do coletivo Anonymous é o que torna o grupo um símbolo perturbador para o governo.

Em reação ao efeito 'pós-LulzSec', o Anonymous vem atuando em consequência de seu ideal revolucionário e resistência, em ações que possam expor informações e dados confidenciais por parte dos governos e corporações – fato que o movimento de hacktivistas desmitificam que "informação privada" e "privacidade" são elementos reais, ao contrário da informação na esfera pública. Esta distinção é um dos fundamentos de um estado neoliberal, o meio pelo qual a individualidade é constituída e monitorada (Coleman, 2012).

1.4 A CULTURA DA TECNOMERITOCRACIA

A ascensão da Internet e das tecnologias de informação trouxe à comunidade virtual novos métodos e práticas em todas as áreas da sociedade civil, incluindo o ativismo, que é afetado de duas maneiras. Em primeiro lugar, as novas tecnologias deram aos manifestantes um meio conveniente e poderoso para disseminar suas mensagens e mobilizar uma ação global (Castells, 2003). Em segundo, as inovações tecnológicas beneficiaram o cidadão comum na capacidade de aplicar ferramentas de *hacking* para conduzir operações cibernéticas análogas aos protestos no espaço urbano. Esta mistura de *hacking* com ativismo, conhecido pelo mix "hacktivismo", tornou-se cada vez mais prevalente, se afirmando relevante em uma resistência popular virtual, fortalecida por esta cultura exclusiva de hackers.

De uma maneira mais categórica, os hackers não são um grupo ideológico. No entanto, a comunidade hacker possui uma história de ativismo político – atuando no hacktivismo - que passou a ser definida na era do WikiLeaks[33]. Se há uma coisa que une hacktivistas através de múltiplas gerações, é a dedicação à ideia de que a informação na Internet deve ser livre e a rede, descentralizada - o primeiro princípio é visto como

[33] Momento que centraliza a questão de uma sólida parceria entre o Anonymous e WikiLeaks: foram extraídos milhares de emails da empresa de segurança Stratfor pelo grupo de hackers e direcionado para a plataforma do WikiLeaks.
Mais do que isso, o grupo se posicionou ao lado de Julian Assange contra a tentativa do Ministério sueco em extraditá-lo para o Reino Unido e deportado para os EUA, onde enfrentariaum julgamento de abuso sexual. O Anonymous atacaram o site do escritório do procurador sueco, presumivelmente como uma espécie de protesto contra a extradição, e lançou ataques de DDoS contra a Visa e Mastercard, quando essas empresas retiraram serviços de pagamentos no site do Wikileaks.

contrapartida nos conflitos contra corporações e governos pelo mundo, o que desencadeou a resistência colaborativa entre a plataforma WikiLeaks e o Anonymous.

Além do trabalho dos hackers, a ética é o terceiro nível significativo da comunidade hacker, que pode ser chamada de *nethic* ou ética na rede (Himenam, 2001). Esta expressão representa a comunidade dos hackers e seu papel na sociedade em rede, no sentido mais amplo com o termo *netiquette*, o que diz respeito aos princípios comportamentais em uma comunicação na Internet, como o “Rule 34”[34].

> A ética hacker descrita é exemplar da "idade de ouro" da pirataria, que coincidiu mais ou menos com a ascensão da computação gráfica na década de 1980, com duração até os anos 1990. Em 1987, a Apple lançou o Apple II, desenvolvido por Steve Wozniak, que Levy considera como um "verdadeiro" hacker. O Apple II representou a ética hacker, porque foi literalmente feito em código aberto. Qualquer um poderia levantar o capô, como um carro, e mexer com a tecnologia; qualquer pessoa poderia reprogramar e torná-lo mais rápido (McLaughlin, 2012, p. 25).

Desta maneira, de acordo com Himenam (2001), nem todos os hackers compartilham os elementos do *nethic*, mas ainda assim esses elementos estão ligados entre si no significado social e relação com a ética hacker, ao que influenciam na cultura meritocrática da comunidade. Embora o termo ‘ética hacker’ tem sido usado pelo menos desde a década de 1960 (Levy, 1984), foi popularizado por Pekka Himanen em seu livro intitulado *The Hacker Ethic* (2001). Nesta obra, Himanen discute a chamada ética hacker e sua relação com o que Manuel Castells cunhou de "O Espírito do Informacionalismo" (Castells, 2003). Por outro lado, Castells atribui suma importância na capacidade humana de produzir inovação quanto à questão de processos colaborativos na comunidade em rede. Neste aspecto, pode-se dizer que os hackers são "produto de um trabalho inteligente, mas de um intelecto coletivo que depende do acesso livre à informação e cooperação mútua” (Castells, 2003, p. 42).

> Nesse sentido restrito, a cultura hacker, a meu ver, diz respeito ao conjunto de valores e crenças que emergiu das redes de programadores de computador que se interagiam online em torno de suas colaborações em projetos autonomamente

[34] Conhecida também como “Regras da Internet" redirecionadas aos memes da internet pelo fórum do 4chan. Ver em: https://en.wikipedia.org/wiki/Rule_34_%28Internet_meme%29. Acesso: 27 de Abril 2016.

> definidos de programação criativa (Levy, 2001). Duas características críticas devem ser enfatizadas: por um lado, a autonomia dos projetos em relação às atribuições de tarefas por instituições ou corporações; por outro, o uso da interconexão de computadores como a base material, tecnológica da autonomia institucional. Visto isso, a Internet foi originalmente a criação da cultura tecnomeritocrática; depois tornou-se a base para sua própria atualização tecnológica através do input fornecido pela cultura hacker, interagindo na Internet (Castells, 2003, p. 38).

Para Pekka Himanem (2001), a ética hacker é a característica cultural da sociedade informacional. Dessa forma, a cultura hacker desempenha um papel fundamental na composição da Internet por duas razões: pode-se sustentar que é o ambiente fomentador de inovações tecnológicas mediante a cooperação e a comunicação livre; é o que faz a ponte entre o conhecimento originado pela cultura tecnomeritocrática. Os hackers, contudo, ilustram um aspecto particular da cultura que é vista como uma subcultura inerentemente ligada a uma cultura parental (Castells, 2003).

A importância dessa parte da cultura da Internet - particularmente nos anos 1980, 1990, e até hoje - para a nova geração é fundamentada em dois fatores. Em primeiro lugar, a cultura da computação gráfica e diversos processo colaborativos, que em muitos aspectos, são vistos como atos de rebeldia uma vez que exigem mudanças constantes em função da evolução de um hardware ou software. Em segundo lugar, o espaço semiótico que a tecnologia apresenta é consideravelmente menos material do que canais tradicionais de expressão. Outro elemento imprescindível para essa dimensão cultural é a iniciativa conjugada por Richard Stallman ao criar a Fundação do Software Livre (Free Software Foundation)[35], em 1985.

> Stallman transformou seu esforço numa cruzada política pela Liberdade de expressão na era do computador, criando a Free Software Foundation (FSF), e proclamando o princípio da livre comunicação e do livre uso do software como um direito fundamental. Criou sozinho o movimento do software gratuito, e tornou-se um dos ícones da cultura hacker. Mas seu desenvolvimento político, por si só, não lhe permitiu remover

[35] Richard Stallman, professor do MIT, havia trabalhado como estudante em projetos onde o software era desenvolvido livremente sem copiar ou modificar suas estruturas. Levando esta ideia ao nível do grupo de pesquisa no MIT, Stallman criou a FSF, partindo para demonstrar que todo um sistema operacional poderia ser desenvolvido e compartilhado livremente. O resultado foi o Unix – assim como o sistema GNU, que, em Agosto de 1996, tornou-se completo pela adição de um núcleo operacional. “The Free Software Foundation: 30 years in” Ver em: https://opensource.com/business/15/9/free-software-foundation-30-years. Acesso: 29 de Abril 2016.

> os imensos obstáculos técnicos que encontrou na criação de um novo Sistema operacional, equivalente ao UNIX, mas diferente dele. Embora a divulgação que ele e sua equipe faziam dos seus esforços pela Net tenha aberto o caminho para o future software de fonte aberta, seu Sistema (HURD) não funcionou efetivamente até 1996 (Castells, 2003, p. 41).

No caso dos hacktivistas do Anonymous, em seu slogan “Nós somos Anonymous. Nós não perdoamos. Nós não esquecemos. Espere por nós” [36], evoca a ameaça onipresente da cultura hacker (Sauter, 2013). Embora os seus métodos, a tática de DDoS, em particular, podem ser bastante simplistas na realidade, consideradas avançadas o suficiente para confundir a maioria da opinião pública, incluindo a aplicação da lei e os meios de comunicação, que são satisfeitos para atribuir o apelido de "hacker" para qualquer prática não convencional como interesse público. A imagem cultural do Anonymous, é assim, uma colaboração entre a comunidade virtual e os meios de comunicação, o que estimula a cultura do hacktivismo no conflito ininterrupto contra a agenda midiática ao relacionar a imagem do movimento alinhada ao estereótipo de cibercriminosos.

Há, no entanto, subculturas hacker construídas sobre princípios políticos bem como sobre revolta pessoal. Richard Stallman considera a busca de excelência tecnológica secundária ao princípio fundamental do software gratuito, que, para ele, é um componente essencial da liberdade de expressão na Era da Informação (Castells, 2003). Neste sentido, Jordan e Taylor (1998) argumentam que a cultura tecnomeritocrática reconhece a diversidade do mundo dos hackers e ao mesmo tempo, une todos os seus membros acima de divisões ideológicas e quanto ao comportamento pessoal: a crença compartilhada no poder da interconexão de computadores e a determinação de manter esse poder tecnológico da computação como um bem comum – pelo menos para a comunidade dos hackers.

Portanto, essa comunidade de hacktivistas carregam características fundamentais comuns. A primeira é o valor da comunicação livre e horizontal. A prática das comunidades virtuais, dos hackers em especial, sintetiza a prática da livre expressão global, numa era dominada por conglomerados de mídias e burocracias governamentais

[36] “We are Anonymous. We do not forgive. We do not forget. Expect us”. – slogan é visto no primeiro vídeo contra a Igreja da Cientologia, em 2008. Ver em: https://www.youtube.com/watch?v=JCbKv9yiLiQ. Acesso: 28 de Abril 2016.

censoras. Assim, embora extremamente diversa em seu conteúdo, a fonte comunitária da Internet a caracteriza de fato como um meio tecnológico para a comunicação horizontal e uma nova forma de livre expressão, que para Castells (p. 49, 2003), "assenta também as bases para a formação autônoma de redes como um instrumento de organização, ação coletiva e construção de significado".

2. UMA CRONOLOGIA DAS OPERAÇÕES

O coletivo Anonymous teve seu ápice há oito anos no fórum mais popular da Internet dos anos 2000, o webblog 4Chan. E são por natureza, indivíduos complexos para serem definidos: sustentam um nome por vários grupos de hackers, entusiastas de tecnologia, ativistas, defensores dos direitos humanos e geeks da informática. A antropóloga Gabriella Coleman (2012) define o coletivo como um conjunto de ideias e ideais adotados por esses hackers e centrados em torno do conceito de anonimato; também suportam a ideia sob ações coletivas online e no mundo real que vão desde brincadeiras formidáveis até ações triviais, como por exemplo, os protestos e campanhas mundiais mediados pelas redes sociais, principalmente a utilização em massa de perfis do Twitter durante o apoio tecnológico para os manifestantes da Primavera Árabe, que culminou em 2010 ao estimular um levante de usuários para as ruas contra governos ditatoriais.

As operações instrumentadas pelo Anonymous, são por vezes pacíficas e legais, ocasionalmente perturbadoras e ilícitas, porém carregadas de uma euforia de revolta que influencia comunidades alternativas pela Internet. Em sua maioria, o Anonymous age assim para promover causas políticas, mas também, por pura diversão. O que começou como uma rede de trolls, tornou-se, na maior parte do tempo, uma força para o bem no mundo; o que começou como uma reação da Igreja da Cientologia, estendeu-se em causas pela liberdade de expressão em países onde as violações de direitos humanos danificavam a sociedade civil pelo Oriente Médio: Tunísia, Arábia Saudita, Síria, Bahrein, Marrocos, Iêmen, Líbia, Líbano, Kuwait e entre outros países árabes corroídos pela ditadura e crise política.

Enquanto o Anonymous não apresenta uma base ofensiva digital que possa desmantelar instituições ou alterar leis injustas, suas operações são vistas na maioria das vezes como simplistas e imprudentes (Coleman, 2014). Para aqueles vestindo a máscara de Guy Fawkes associados com grupo Anonymous, são indivídus recebidos como a promessa idealizadora da Internet, e isso influenciou na troca do individualismo para o coletivismo.

> As defenders of digital rights, I think Anonymous is the perfect 'group' to fight for Internet freedom. Anons typically spend a majority of their waking hours (and some of their sleeping hours) online and many have careers in IT, which makes them much more intimately in tune with what will work best for the Internet. I, among others, helped physically shield Aaron Swartz's funeral from impending threat of protest by Westboro Baptist Church. During this whole time, my interest and passion for the Linux operating system grew. I shared most of the knowledge I found while learning Linux under the hashtag #OpNewBlood to help other n00bz learn also. I like to think my biggest contribution has been to help people learn how to use their system and hopefully be a little safer/more private when they do.[37]

No entanto, é importante lembrar que o Anonymous funciona como uma colméia; um por todos e todos por um. Mas, em quais aspectos suas ações puderam contribuir para o legado do ativismo digital contemporâneo? Suas operações sempre serão influenciadas pelo passado durante a 'Era do Lulz'. O hacktivismo do grupo Anonymous pode ser visto como exemplo da forma como as ferramentas virtuais que enviam ao mundo real um caos através de uma consciência coletiva implacável (McLaughlin, 2012).

2.1.1 Operacão Chanology – 2008

Em janeiro de 2008, o site de notícias Gawker publicou um vídeo[38] em que Tom Cruise entusiasticamente elogia os benefícios da Igreja da Cientologia, o que era pra ser uma publicidade positiva, foi vista como um mecanismo controverso para a entidade.

---

[37] Tradução nossa: Como defensores de direitos digitais, acho que Anonymous é o "grupo" perfeito para lutar pela liberdade na Internet. Anons normalmente gastam maioria de suas horas acordados (e algumas de suas horas de sono) on-line e muitos têm carreiras em TI, o que os tornam mais intimamente em sintonia com o que irão fazer de bom para a Internet. Eu, entre outros, ajudei a proteger fisicamente o funeral de Aaron Swartz da iminente ameaça de protesto de *Westboro Baptist Church*. Durante todo este tempo, meu interesse e paixão pelo sistema operacional Linux cresceu. Eu compartilhei a maior parte do conhecimento que encontrei ao mesmo tempo aprendendo sobre o Linux sob a hashtag #OpNewBlood para ajudar outros novatos a aprender também. Gosto de pensar que a minha maior contribuição tem sido ajudar as pessoas no aprendizado de sistemas e softwares, e espero que tenham um pouco mais de segurança e privacidade quando utilizarem. " – Resposta do 'Anon' Pr1m1t1v3, em 13 de Abril de 2016, via e-mail.

[38] O vídeo publicado no site Gawker - http://gawker.com/5002269/the-cruise-indoctrination-video-scientology-tried-to-suppress. Acesso: 07 de Maio 2016.

Com isso, o vídeo foi protegido por direitos autorais e por isso, a Igreja envia uma carta de ameaça para a equipe de jornalismo do Gawker, como um pedido de remoção do vídeo. Logo, o coletivo Anonymous, depois de observar as demandas autoritárias da igreja como tentativas de censura, um dos usuários que acompanhavam o momento no 4Chan se exaltava: "Eu acho que é hora do /b/ fazer algo grande. Estou falando de hackear ou derrubar o website oficial da Cientologia".

Depois do grupo de hackers se declararem coletivamente contra o ato da Igreja através do 4Chan, um membro do Anonymous divulga no YouTube uma espécie de comunicado de imprensa que incluía imagens audiovisuais de nuvens e tempestades, com uma voz computadorizada em padrão narrativo no fundo do vídeo: "Vamos proceder com o plano em expulsar vocês da Internet e sistematicamente desmantelar a Igreja da Cientologia", disse a voz. "Vocês não têm nada a esconder."[39] Em poucas semanas, o vídeo no YouTube foi visto por mais de dois milhões de usuários.

Nesse processo, o Anonymous já havia superado o 4chan. Os hackers começaram a se reunir em canais do IRC para coordenar táticas. Ao adotar ataques de DDoS, fizeram com que o site principal da Cientologia ficasse offline durante dias. Logo, começaram a desenvolver mecanismos para destruir o discurso da Igreja na Internet. O grupo então criou um *Google bomb*, de modo que uma busca no Google por "seita perigosa" renderia ao site da Cientologia o topo da página de resultados do buscador. Outros enviaram centenas de pizzas à instituições da Cientologia pela Europa e para a sede de Los Angeles. Mas seus líderes, que também haviam recebido ameaças de morte, decidiram denuncá-los ao FBI c investigação dos hacktivistas.

> Anonymous's willingness to wreak havoc in pursuit of lulz, but also in defense of free speech and in opposition to the malfeasances and deceptions of Scientology, calls to mind the nineenth-century European “social bandits” described by historian Eric Hobsbawm in his 1959 book Primitive Rebels. These bandits are members of mafias, secret societies, religious sects, urban mobs, and outlaw gangs; they are ultimately thugs, but, according to Hobsbawm, they nurture a faintly revolutionary spirit: often when they plunder they also redistribute goods to the poor, or offer them protection against other bandits (Coleman, 2012, p. 24). [40]

[39] O press-release contra a Igreja da Cientologia divulgado no YouTube, em 2008 - https://www.youtube.com/watch?v=JCbKv9yiLiQ. Acesso: 07 de Maio 2016

[40] Tradução nossa: O Anonymous se dispõe a causar estragos em busca do lulz, mas também em defesa da liberdade de expressão e em oposição às malfeitorias e enganos da Cientologia, o que lembra o termo europeu do século 19 "bandidos sociais", descrito pelo historiador Eric Hobsbawm em sua obra de 1959,

Em 15 de março de 2008, milhares de Anons decidiram concretizar o que tanto discutiam na Internet sobre liberdade de expressão: membros do coletivo ao redor do mundo saíram pelas ruas com placas e cartazes de protesto contra a Igreja da Cientologia e se posicionaram nas sedes das principais capitais, de Londres a Sydney. Em sintonia com o contexto do anonimato, os organizadores decidiram que todos os manifestantes deveriam usar a mesma máscara. Depois de até considerarem o herói dos quadrinhos Batman, definiram sair às ruas com a máscara de Guy Fawkes, como um tributo ao filme do personagem de Alan Moore, "V de Vingança", uma obra distópica de 2005. "A ação foi concentrada em todas as grandes cidades, em uma quantidade extraordinária", responde Gregg Housh, um dos organizadores do protesto durante o documentário 'Nós Somos Legião'[41]. O grupo de hacktivistas do Anonymous trabalharam nessa operação no sentido de encontrar um estilo nodatamente público (Sauter, 2014).

Logo após ataques de DDoS e brincadeiras, o Anonymous começou a redirecionar suas táticas, a partir do momento em que divulgam fatos controversos sobre a Cientologia, destacando o uso da censura pela igreja e o abuso dos direitos humanos. Com isso, o Anonymous havia se deslocado de seu santuário virtual e disposto a mudar o mundo.

2.1.2 Operação PayBack - 2010

Membros do coletivo propuseram uma ação chamada *OpPayBack*. Como a jornalista Parmy Olson mencionou em seu livro, "Nós Somos Anonymous" (2012), a *Operation Payback* começou em forma de campanha de apoio a sites de compartilhamento de arquivos como o The Pirate Bay, conhecido como sucessor do Napster, mas o foco foi logo ampliado com discurso político.

Primitivos Rebeldes. Estes bandidos são membros de máfias, sociedades secretas, seitas religiosas, mobilizações urbanas e gangues fora da lei; eles (o Anonymous) são, em última análise, bandidos, mas, de acordo com Hobsbawm, eles também nutrem um espírito vagamente revolucionário: muitas vezes quando eles 'saqueam', também redistribuem bens aos pobres, ou lhes oferecem proteção contra outros fora da lei.

[41] "We Are Legion: The Story of the Hacktivists" é um documentário lançado em 2012 sobre o funcionamento e as crenças do coletivo hacktivista Anonymous, demonstrando suas ações desde integrações virtuais via 4Chan até a Primavera Árabe, de 2011. O documentário pode ser assistido aqui: https://www.youtube.com/watch?v=d-_2z8QlC1o.

No final de 2010, a pedido do Departamento de Estado nortet-americano, várias empresas, incluindo MasterCard, Visa e PayPal, interromperam seus serviços de doações direcionadas ao WikiLeaks, a organização de denunciantes que havia publicado 250 mil telegramas diplomáticos dos Estados Unidos. Em um vídeo, os hacktivistas do Anonymous lançam ação de vingança, prometendo atacar as empresas que haviam impedido o WikiLeaks de receber doações. Durante a *OpPayBack*, no início de dezembro, o Anonymous estabeleceu um plano de recrutamento de usuários que pudessem auxiliar na ação, através do direcionamento de mensagens e instruções online de como realizar DDoS em grande escala.

> Hundreds of people flooded its chatrooms and its operators directed them to download a piece of software that they could use to "DDoS" (or "denial-of-service attack") PayPal's website: effectively flood it with traffic and render it useless, or as they put it: "HOW TO JOIN THE FUCKING HIVE".[42]

Dois anos depois da Operação Chanology ser lançada, um grupo diferente de Anons iniciaram uma segunda onda[43] da OpPayBack, mais uma vez sem planejamento. De acordo com uma fonte do Anonymous, a iniciativa foi organizada pelo IRC do AnonOps[44], difundido em blogs, no 4chan, Twitter, e, finalmente, chegando à mídia convencional. Graças à tempestade política causada pelo vazamento de milhares de telegramas do WikiLeaks sobre crime de guerra no Iraque e Afeganistão, o AnonOps foi capaz de comandar uma infantaria de ativistas para paralisar os sites do PayPal e Mastercard, por meio do LOIC (Coleman, 2012). "Um pessoal da grande imprensa já havia notado o que estava ocorrendo e dentro de algumas horas, a ação se tornou viral",

[42] Tradução nossa: Centenas de pessoas inundaram as salas de chat e os administradores dando instruções para baixar um software que os usuários poderiam usar para "DDoS" (ou "ataque de negação de serviço") no website do PayPal: efetivamente inundando com o tráfego e tornando-o inútil, ou como eles dizem: "como participar da MALDITA OPERAÇÃO". Ver em: https://www.theguardian.com/technology/2013/aug/18/we-are-anonymous-parmy-olson-review . Acesso: 12 de Maio 2016.

[43] Ataques da 'Operation Payback' miram os sites da MasterCard e PayPal para vingar o WikiLeaks - http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks/?_r=0. Acesso: 15 de Maio 2016.

[44] AnonOps era uma rede de IRC criado pelo jornalista e Anonymous Barrett Brown no final dos anos 1980. O canal havia se tornado o centro das atenções da mídia como uma organização sem liderança, inicialmente frequentado por apenas hackers.

recordou um membro do Anonymous que se responsabilizou pelo ataque. "Ficamos atordoados e um pouco com medo, para ser honesto."

> While we don't have much of an affiliation with WikiLeaks, we fight for the same reasons. We want transparency and we counter censorship. The attempts to silence WikiLeaks are long strides closer to a world where we cannot say what we think and are unable to express our opinions and ideas. We cannot let this happen. This is why our intention is to find out who is responsible for this failed attempt at censorship. This is why we intend to utilize our resources to raise awareness, attack those against and support those who are helping lead our world to freedom and democracy.[45]

Durante dias, a Operação Payback fez com que sites da Visa, MasterCard e PayPal ficassem desconectadas após fase de desconfiguração em consequência dos efeitos da ação de boicote contra o WikiLeaks. Logo após repercussão mundial, em documentos judiciais, o PayPal afirmou que os ataques custaram à companhia mais de cinco milhões de dólares. Em uma manchete do Huffington Post, era destacado "Visa DOWN"[46], o que dada as circunstâncias do ativismo caótico ilustrado pelo coletivo, um exultante Anon publica no Twitter de maneira comemorativa: "Liberdade de expressão não tem preço. Para todo o resto, existe Mastercard".

---

[45] Mensagem publicada em 2011, em um dos sites do grupo para justificar seus ataques às instituições financeiras do PayPal e Mastercard. Tradução nossa: Embora não tenhamos uma afiliação com o WikiLeaks, lutamos pelas mesmas razões. Queremos transparência e combater a censura. As tentativas de silenciar o WikiLeaks são longos passos perto de um mundo onde não podemos dizer o que pensamos e que somos incapazes de expressar nossas opiniões e ideias. Não podemos deixar que isso aconteça. É por isso que a nossa intenção é descobrir quem é responsável por esta falha tentativa de censura. É por isso que temos a intenção de utilizar nossos recursos para aumentar a conscientização, atacar aqueles contra e apoiar aqueles que estão ajudando a levar nosso mundo para liberdade e democracia.

[46] Matéria sobre a repercussão das desconfigurações em massa de sites relacionados com a Visa, parte da OpPayBack - http://www.huffingtonpost.com/2010/12/08/visa-down-wikileaks-suppo_n_794039.html. Acesso em: 14 de Maio 2016.

Figura 1: Um perfil do Anonymous anuncia o sucesso da operação PayBack

É incontestável que a Operação PayBack foi originalmente motivada pelas ações de milhões de usuários que se interconectavam ao mesmo tempo no fórum do 4chan, com a intenção de se instruir e vivenciar as ações de ativismo digital. Portanto, o princípio básico subjacente era a mesma ética hacktivista de motivar uma defesa do WikiLeaks: a informação quer ser livre[47]; e não deve ser acumulada por estados governamentais poderosos, nem mesmo estar sob o controle de interesses comerciais (Assange, 2013).

2.1.3 Operação Primavéra Árabe – 2011

Para Christina Grammatikopoulou (2014), o hacktivismo político possui alcance indefinido sobre a adoção de métodos baseados nos atos associados à ferramentas de computação e algorítimos, parte de uma cultura especializada e sólida construída no ciberespaço, pelos hackers da computação do século 21.

> In this process they often used similar means to express their discontent against inequality and exploitation: by reclaiming the public space, sharing slogans with the other protesters, hiding behind the same "Anonymous" masks. The homogenization of the visual and verbal expression of the revolts is intrinsically

[47] "A informação quer ser livre", Stewart Brand, 1984.

linked to the reflection of these movements on the digital media and the social networks (Grammatikopoulou, 2014, p. 204).[48]

Portanto, até o final de janeiro de 2011, o coletivo Anonymous pareciam estar dedicados inteiramente à campanhas ativistas, em detrimento da formação de ramificações que buscavam introduzir novos meios de hacktivismo com as próprias mãos, como o AntiSec, GhostSec, entre outros (Coleman, 2012). Em consequência disso, alguns Anons ainda lamentavam o fim da era do 'lulz', embora muitos foram revigorados pela contribuição em massa do movimento com a derrubada histórica de regimes ditatoriais no Oriente Médio.

A repercussão midiática sobre os vazamentos de telegramas do WikiLeaks ainda era um problema para alguns regimes governamentais. Após bloqueio do WikiLeaks na Tunísia, o Anonymous anunciava a *OpTunisia* em Janeiro de 2011; em meio tempo para divulgação do ato, o canal AnonOps embarcou em uma série de campanhas para promover liberdade de expressão em apoio à Primavera Árabe. O procedimento inicial do movimento foi o ataque à sites do governo tunisiano e, eventualmente, a atuação como grupo de defesa de direitos humanos a partir da orientação aos cidadãos para contornar a censura e escapar da vigilância eletrônica, por meio de kits virtuais de cuidado, como por exemplo, tutoriais e guias como utilizar o VPN (Virtual Private Network) e se concetar à rede de anonimato Tor.

[48] Tradução nossa: Nesse processo, eles (hackers) muitas vezes utilizam meios semelhantes para expressar seu descontentamento contra a desigualdade e exploração: com a reivindicação do espaço público, o compartilhamento de slogans com outros manifestantes esconde-se por trás das mesmas máscaras como "Anonymous". A homogeneização da expressão visual e verbal das revoltas está intrinsecamente ligado à reflexão destes movimentos na mídia digital e as redes sociais.

Figura 2: Como Protestar Inteligentemente - Guia enviado pelo Anonymous para os manifestantes

Neste kit[49], os hackers do Anonymous anexam uma mensagem de urgência e motivadora para elucidar o papel da mídia social aos manifestantes: "Esta é a sua revolução. Ela não será televisionada, nem tweetada ou comentada no IRC. Vocês devem sair às ruas ou irão perder a luta". Embora a contribuição pelo Anonymous fora inevitavelmente ovacionada, a queda histórica dos regimes ditatoriais no Oriente Médio aconteceu em um efeito dominó. Porém, para uma minoria do coletivo, poderia haver nenhuma evidência mais clara de uma ascendência dos chamados “moralfags”[50] (Coleman, 2012).

[49] O kit de segurança do Anonymous foi composto por múltiplas páginas, descrevendo como se proteger durante os protestos e no meio virtual, para que fosse possível alertar o mundo em tempo real sobre o momento histórico da Primavera Àrabe. Os documentos foram traduzidos pela equipe do veículo *The Atlantic* - http://www.theatlantic.com/international/archive/2011/01/egyptian-activists-action-plan-translated/70388/. Acesso: 16 de Maio 2016.

[50] Mencionado em seu último livro, “The Many Faces of Anonymous” (2014), Gabriella Coleman expõe que o coletivo vem gerando mudanças pertinentes ao hacktivismo por diversão, geralmente à custa de

2.1.4 Operação HBGary – 2011

Em fevereiro de 2011, Aaron Barr, CEO da empresa de segurança HBGary, afirmou ter descoberto as verdadeiras identidades por trás dos membros operacionais do coletivo. A princípio, como um contra-ataque padrão, os Anons hackearam o perfil de Barr no Twitter para publicar insultos e piadas preconceituosas contra comunidades de direitos raciais e de LGBT. Após repercussão do conteúdo compartilhado por milhões na rede social, o coletivo parte para uma segunda etapa da operação: o hacking dos servidores da HBGary, ao operar o download de 70.000 e-mails, arquivos e dados de inteligência que foram apagados e por último, a eliminação em massa de conteúdo dos dispositivos iPhone e iPad de Aaron Barr. O trajeto final era tornar público todos os logs de comunicação de Barr, o que surpreendeu diversos setores e autoridades governamentais[51].

> Some Anons took issue with the collateral damage wrought by Operation HBGary, especially the excessive leaking of personal information. The necessarily clandestine nature of such hacks was also criticized by those who saw it as counter to the ethos of transparency. At the time, however, most Anons were thrilled: they had not become Human Rights Watch; the pursuit of a more "mature" agenda did not mean an end to lulz (Coleman, 2012, p. 91).[52]

O que podemos notar sobre o Anonymous até aqui é que desde 2008, o grupo se tornou um gateway político para geeks dispostos a tomar medidas furtivas e aguçadas

---

outros membros vistos como "fags", e outros que constuman insinuar ativismo político, sendo chamados de "moralfags".

[51] Log do canal IRC AnonOps, onde Barr se manifesta com um grupo do Anonymous sobre a repercussão e contato constante com o FBI e a mídia, em Fevereiro de 2011 - http://pastebin.com/p8Pt60Fu. Acesso: 18 de Maio de 2016.

[52] Tradução nossa: Alguns Anons tiveram problemas com os danos colaterais causados pela Operação HBGary, especialmente com o vazamento excessivo de informações pessoais. A natureza necessariamente clandestina desse hacking também foi criticado por aqueles que o viam como contrário quanto ao caráter da transparência. Na época, no entanto, a maioria dos Anons ficaram emocionados: eles não tinham se tornado a Human Rights Watch; a busca de uma agenda mais "madura" não significa o fim do lulz.

pela curiosidade em estabelecer um equilíbrio na Internet, na defesa pela transparência de informação. Para a pesquisadora Molly Sauter (2013), entre outras oportunidades, o Anonymous oferece possibilidades de micro-protesto discretos que não são de algum modo frequente, visto que ainda é uma chance de outros indivíduos fazerem parte de algo maior.

This domain has been seized by Anonymous under section #14 of the rules of the Internet.

Greetings HBGary (a computer "security" company),

Your recent claims of "infiltrating" Anonymous amuse us, and so do your attempts at using Anonymous as a means to garner press attention for yourself. How's this for attention?

You brought this upon yourself. You've tried to bite at the Anonymous hand, and now the Anonymous hand is bitch-slapping you in the face. You expected a counter-attack in the form of a verbal brawl (as you so eloquently put it in one of your private emails), but now you've received the full fury of Anonymous. We award you no points.

What you seem to have failed to realize is that, just because you have the title and general appearence of a "security" company, you're nothing compared to Anonymous. You have little to no security knowledge. Your business thrives off charging ridiclous prices for simple things like NMAPs, and you don't deserve praise or even recognition as security experts. And now you turn to Anonymous for fame and attention? You're a pathetic gathering of media-whoring money-grabbing sycophants who want to reel in business for your equally pathetic company.

Let us teach you a lesson you'll never forget: you don't mess with Anonymous. You especially don't mess with Anonymous simply because you want to jump on a trend for public attention, which Aaron Barr admitted to in the following email:

"But its not about them...its about our audience having the right impression of our capability and the competency of our research. Anonymous will do what every they can to discredit that. and they have the mic so to speak because they are on Al Jazeeera, ABC, CNN, etc. I am going to keep up the debate because I think it is good business but I will be smart about my public responses."

You've clearly overlooked something very obvious here: we are everyone and we are no one. If you swing a sword of malice into Anonymous' innards, we will simply engulf it. You cannot break us, you cannot harm us, even though you have clearly tried...

You think you've gathered full names and home addresses of the "higher-ups" of Anonymous? You haven't. You think Anonymous has a founder and various co-founders? False. You believe that you can sell the information you've found to the FBI? False. Now, why is this one false? We've seen your internal documents, all of them, and do you know what we did? We laughed. Most of the information you've "extracted" is publicly available via our IRC networks. The personal details of Anonymous "members" you think you've acquired are, quite simply, nonsense.

So why can't you sell this information to the FBI like you intended? Because we're going to give it to them for free. Your gloriously fallacious work can be a wonder for all to scour, as will all of your private emails (more than 66,000 beauties for the public to enjoy). Now as you're probably aware, Anonymous is quite serious when it comes to things like this, and usually we can elaborate gratuitously on our reasoning behind operations, but we will give you a simple explanation, because you seem like primitive people:

You have blindly charged into the Anonymous hive, a hive from which you've tried to steal honey. Did you think the bees would not defend it? Well here we are. You've angered the hive, and now you are being stung.

It would appear that security experts are not expertly secured.

```
We are Anonymous.
We are legion.
We do not forgive.
We do not forget.
Expect us - always.
```

Figura 3: Mensagem anexada no site da empresa HBGary

Diante disso, um pequeno grupo de hackers do Anonops havia começado com plano de retaliação e consequentemente expuseram o que parecia ser uma conspiração tão contundente que os membros do Congresso solicitaram uma comissão de investigação contra as ações. Tendo em conta que estas empresas eram privadas, as provas obtidas pelos usuários hackers do AnonOps nunca poderiam ser adquiridas por fins legais, até como um pedido da Legislação sobre Liberdade de Informação[53]. Mais recentemente, o Anonymous tem agido ocasionalmente para expor falhas de segurança e acesso a informações sensíveis, ao optar por desfigurar e enviar spams por e-mail (Sauter, 2012).

> Na realidade, eles ainda não sabiam que Barr estivera propondo uma campanha caluniosa contra sindicato trabalhistas e o WikiLeaks para uma agência governamental e um importante banco. A motivação do grupo era a vingança e o desejo, intensificado pela psicologia coletiva, de perseguir qualquer um que parecesse merecer. À medida que mais e mais pessoas vasculhvam e-mails de Barr e descobriam o que ele fizera com a Hunton & Williams, o ataque repentinamente passou a parecer mais do que justificado, quase necessário para eles. Na comunidade do Anonymous, Sabu, Kayla, Topiary e os outros se tornariam heroicos condutores de justiça vigilante. Barr tinha merecido. Provocara um mundo em que insultar, mentir e roubar eram coisas corriqueiras. Um mundo que trazia emoções eufóricas, diversão e realização, sem praticamente quaisquer consequências no mundo real (Olson, 2014, p. 29).

De maneira notória, em meio a um ácumulo de informações obtidas da HBGary, o Anonymous revela um documento intitulado como "A Ameaça WikiLeaks"[54], que descreve como a HBGary Federal e outras empresas de segurança planejavam prejudicar o WikiLeaks por meio da utilização de documentos falsos para publicação no site. Havia também a evidência de planos que visavam arruinar as carreiras de apoiadores da organização WikiLeaks, entre eles estava o jornalista do veículo The Intercept, Glenn Greenwald e membro do projeto da rede de anonimato TOR, Jacob Appelbaum.

---

[53] Freedom Of information Act, FOIA – Lei que lhe dá o direito de acesso a informações do governo federal. É muitas vezes descrita como a lei que mantém os cidadãos em saber sobre seu governo. Ver em: http://www.foia.gov/. Acesso: 23 de Maio 2016.

[54] Relatório do WikiLeaks sobre o “The WikiLeaks Threat” - https://wikileaks.org/IMG/pdf/WikiLeaks_Response_v6.pdf. Acesso: 16 de Maio 2016.

Para Sauter (2012), o episódio da Operação HBGary é um exemplo de que as dinâmicas do coletivo hacktivista são inerentes a uma dialética entre a criação de poder centralizado e sua dispersão, o que é comum entre comunidades colaborativas da cultura geek e hacker. A relação desconfortável entre essas duas tendências é parcialmente esclarecida quando Anons constantemente lembram um ao outro que se abstenham de se comportar como um líder, e, assim, estimular os membros a buscar o consenso como o modo preposto de tomada de decisão do movimento.

2.1.5 Operação BART – 2011

Todo o engajamento com ações de ativismo digital pelo Anonymous, desde o início, tem deixado a mídia internacional desorientada, especialmente porque a cobertura dos veículos de imprensa foram afetadas ao colocar à frente das repercussões, manchetes controversas sobre o Projeto Chanology, Operação HBGary, e a Operação BART, lançada contra a agência de transporte de São Francisco depois de bloquearem o de serviço telefonia celular nas estações de trem que interceptavam um protesto planejado contra a violência policial.

Neste contexto, Levy (2012) relaciona a ética hacker como uma configuração aprimorada da ideia de que sistemas descentralizados devem ser trabalhados de forma coletiva e destinada a articular uma ação, objetivo e solução para um problema. Outra situação relacionada às operações de retaliação coletiva é descrita por Levy em “Heróis da Revolução”, sobre o hacker ‘Greenblatt’, conhecido como Stewart Nelson, ao que demonstra seu interesse pela ética hacker quanto à domínios eletrônicos inexplorados – na busca por vulnerabilidades em sistemas de comunicação em companhias de telefonia -, ainda na década de 1963. Nelson acreditava que usufruía de uma Ética Hacker mais ampliada , afirmando que “se nós agirmos por nossa própria iniciativa para trabalhar, vamos descobrir mais, produzir mais e estar mais no controle” (Levy, 2012, p.82).

"Sooner or later the people in this country gotta realize the government
does not give a fuck about them. The government doesn't care about you, or your children,
or your rights, or your welfare, or your safety, it simply doesn't give a fuck about you.
It's interested in its own power, that's the only thing, keeping it and expanding it wherever possible."

//
#OpBart #Bart-Action #FREETOPIARY #FREEMERCEDES #FREEBRADLEYMANNING #Justice for Oscar Grant
No Justice, No Bart ### UA In The Bay ### Bay Of Rage ### Anti-sec #Justice for Charles Hill
//

//
Your Website has been hacked and database has been leaked by:
#t0nicwater #Bl4ckAbby #NaDa #Tanko #Anonymous #hackers
//

Dear Bay Area Rapid Transit, The People and All Government Agencies,

We are Anonymous, we are your citizens, we are the people, WE DO NOT TOLERATE OPPRESSION FROM ANY GOVERNMENT AGENCY.
BART has proved multiple times that they have no problem exploiting and abusing the people.
First they displayed this by the two recent killings by BART police. Under no circumstance, unless police are shot at,
make police killings acceptable. Non-lethal weapons were available to use during both incidents,
providing even that was necessary, but instead they shot to kill. Next they violated the people's right to assembly and prevented
other bystanders from using emergency services by blocking cell phone signals in order to stop a protest against the BART police murders.
Lastly, they set up this website called mybart.gov and they stored their members information with virtually no security.
The data was stored and easily obtainable via basic sqli. Any 8 year old with a internet connection
could have done what we did to find it. On top of that none of the info, including the passwords,
was encrypted. It is obvious BART does no give a fuck about its customers, funders and tax payers,THE PEOPLE.

The governments and government agencies of the world are becoming tyrannical and oppressive,
and the people are responding and will not take your shit for much longer. The people will fight
this oppression with protests, demonstrations, riots, hacking, ddos, online attacks and by any other means.
We will not allow ourselves to be killed, exploited, or get shitted on. From the streets of Chile,

Figura 4: Mensagem anexada após o Anonymous derrubar o sistema do BART

Em consequência disso, o grupo de hackers revela em comunicado de imprensa suas motivações ao desaprovar as ações do BART contra os manifestantes nas áreas do sistema de transporte público de São Francisco: "Durante os protestos, vimos pessoas sendo reprimidas, e mais uma vez, o Anonymous tentará mostrar àqueles que praticam a censura o que é ser silenciado. A #OpBART É uma operação voltada para o equilíbrio - e aprendizagem. Vocês censuram as pessoas porque elas desejam se expor contra as injustiças que ocorrem ao seu redor. O BART tomou a decisão consciente de ordenar empresas de telefonia celular a encerrarem seus serviços no centro da cidade, inibindo os cidadãos na área das estações do uso de telefones celulares, até mesmo em caso de emergência.

> And Anonymous is organized not only around a radical democratic (at times chaotic and anarchic) structure but also around the very concept of anonymity, here constituted as collectivity. The accumulation of too much power – especially in a single point in virtual space – and prestige is not only taboo but functionally very difficult. The lasting effect of Anonymous may have as much to do with facilitating alternative practices of sociality – upending the ideological divide between

> individualism and collectivism – as with attacks on monolithic banks and sleazy security firms (Coleman, 2012, p. 95).[55]

Para Coleman (2012), o Anonymous se tornou um paradoxo da era da informação: uma causa célebre em oposição à notoriedade. Porém, poucos Anons foram encorajados em revelar suas identidades, apesar da solicitude e pressão dos veículos de mídia. Ao mesmo tempo, o Anonymous conseguiu difundir a sua mensagem da maneira mais ampla possível, por todos os canais de mídia à sua disposição - em contraste com os grupos de ciberterrorismo que buscam permanecer ocultos a qualquer custo.

No entanto, devido à distribuição de hospedagem utilizada pelo BART, a parte de DDoS da operação não obteve sucesso. "Vocês não podem fazer DDoS de rede de “Cloud Hosted Network"[56], um participante da operação explicou ao grupo. De acordo com anúncios do grupo que antecederam ao ato, a Operação BART consistia em táticas de envio massivo de spam para o sistema de caixa de entrada do BART e fax com onda de e-mails contendo mensagens que condenavam a força policial de São Francisco, incluindo o sobrecarregamento do servidor por meio de ataques DDoS e organizando protestos pelas redes sociais no Civic Center[57], em São Francisco. O plano foi anunciado por meio de perfis de Twitter vinculados ao Anonymous, bem como um vídeo publicado no YouTube.

> To the people of San Francisco, we invite you to join us Monday, August 15th, at 5pm, for a peaceful protest at Civic Center Station. We will show the world and BART that we will

---

[55] Tradução nossa: E o Anonymous é organizado não só em torno de uma estrutura radical democrática (às vezes caótica e anárquica), mas também em torno do próprio conceito de anonimato, aqui constituída como coletividade. A acumulação de poder demasiado - especialmente em um único ponto no espaço virtual - e prestígio não apenas tabu, mas funcionalmente muito difícil. O efeito duradouro do Anonymous pode ter tanto a have em facilitar práticas alternativas de sociabilidade - derrubando a divisão ideológica entre o individualismo e coletivismo - como com ataques a bancos monolíticos e empresas de segurança.

[56] A nuvem de hospedagem fornece configuração para sites em servidores virtuais que movimentam seus recursos de conexão a partir de extensas redes subjacentes de servidores físicos. O Cloud Hosting segue o modelo de utilidade de computação na medida em que está disponível como um serviço e não produto e é, portanto, comparável com utilitários tradicionais, tais como a eletricidade e o gás. Ver em: http://www.interoute.com/what-cloud-hosting. Acesso: 22 de Maio 2016.

[57] O Centro Cívico de São Francisco é um conjunto de escritórios do governo local, estadual e federal, que contém as maiores instituições governamentais e culturais da cidade. Ver em: https://sfciviccenter.org/. Acesso: 23 de Maio 2016.

> not stand for these types of actions. We encourage you to wear a red shirt, in remembrance of those who have been battered by the BART police. We also encourage you to bring cameras to record any further abuse by police, and to legitimize the protest. Remember to bring your mask, and remember that this is a peaceful protest. Anonymous does not support violent action and it is discouraged.[58]

Em 14 de agosto, o Anonymous decidiu divulgar dados pessoais de pelo menos de 2.400 agentes do BART, incluindo seus nomes, e-mails, senhas, números de telefone e endereços, estabelecida como uma resposta direta contra a decisão do BART no bloqueio dos sinais de dispositivos móveis no metrô, por meio da plataforma Pastebin. O Anonymous, ao ver que os ataques acabaram por ser ineficazes na conclusão da operação, os hackers fizeram uma tentativa em forma de teste nos sites comerciais do BART, como myBART.com, implementando a assinatura da máscara de Guy Fawkes e bandeiras de pirata na página inicial.

Enquanto isso, o Anonymous e outros manifestantes contra o BART planejavam mais uma demonstração pública durante o trajeto do período de fim de expediente, em em 22 agosto de 2011. No final de semana, perfis de Twitter dos hacktivistas encorajaram seguidores a aderir ao protesto na estação do Civic Center. Hashtags como #OpBART e #MuBARTek foram vestígios de que a operação estava cada vez mais popular e efetiva.

[58] O vídeo pode ser visto no link https://www.youtube.com/watch?time_continue=80&v=o10k3M0-L9E. Acesso: 23 de Maio 2016.

Figura 5: Anúncio da segunda parte da #OpBART

2.1.6 Operação Megaupload – 2012

O cenário do hacktivismo que se forma através do contato direto entre ativistas hackers oferece casos pertinentes a uma demonstração que localiza as operações de ativismo digital na tradição de desobediência civil (Samuel, 2014). Paralelo à isso, Castells (2013) afirma que o fenômeno do hacktivismo é visto como uma sincronia de atividades conduzidas pela apropriação descentralizada do ciberespaço, em diferentes lugares e indivíduos mas na busca pelos mesmos fins.

Nesta circunstância, em 2012, a Operação Megaupload foi notória como uma camapanha voltada para ações de DDoS e protestos em massa pelas mídias sociais, em retaliação do encerramento do serviço de hospedagem de arquivos Megaupload[59],

[59] Megaupload Ltd. foi uma empresa online com base em Hong Kong, estabelecida em 2005, pelo Neozelandês Kim Dotcom (originalmente Kim Schmitz). Em janeiro de 2012, a polícia da Nova Zelândia invadiu sua casa em Auckland e colocou-o sob custódia em resposta às acusações norte-americanas. Dotcom foi acusado de ter custado à indústria do entretenimento $ 500 milhões por meio de conteúdo não licenciado enviados nos servidores do Megaupload, com 150 milhões de usuários registrados. Embora

diretamente ordenado pelo Departamento de Justiça dos EUA, em Janeiro de 2012. Neste mesmo dia, dez perfis da indústria musical e sites governamentais teriam sido derrubados, momento descrito como "um dos maiores ciberataques em uma escala jamais realizada" pelo perfil de Twitter do AnonOps.

Figura 6: Perfil do AnonOps anunciando ataques pelo Twitter

O pedido de bloqueio era constituído por acusações de violação de direitos autorais e conspiração por lavagem de dinheiro[60]. Como parte da repressão, dezenas de mandatos de prisão foram executados nos EUA e em oito países pela Europa, Hong Kong e na Nova Zelândia. Após poucas horas do anúncio sobre a acusação, a página inicial do Departamento de Justiça dos EUA permaneceu fora do ar por longo período. Nesse cenário, os membros do Anonymous decidiram divulgar um comunicado sobre o encerramento do Megaupload e lançamento oficial da campanha conhecida como Operação Megaupload – com a hashtag #OpMegaupload - via Pastebin:

uma ação judicial esteja ainda em curso sobre o Megaupload, em janeiro de 2013, Dotcom lançou outro serviço de armazenamento em nuvem chamado Mega, com estrutura de criptografia para impedir que o governo ou terceiros invadam a privacidade dos usuários. Ver em: https://www.vice.com/video/kim-dotcom-the-man-behind-mega. Acesso: 24 de Maio 2016.

[60] "Megaupload shutdown: guns, cars and cash seized in police swoop": https://www.theguardian.com/technology/2012/jan/20/megaupload-shutdown-guns-cars-cash-seized. Acesso: 24 de Maio 2016.

> O site popular de compartilhamento de conteúdo, megaupload.com, é bloqueado pela justiça dos EUA – FBI e acusa seu fundador de violar as leis de pirataria. Quatro membros do seviço Megaupload também foram presos. O FBI divulgou um comunicado de imprensa em seu site que você pode ver aqui: http://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-with-widespread-online-copyright-infringement
> Nós do Anonymous estamos lançando o nosso maior ataque em sites de toda a indústria da música e do governo. Lulz. O FBI não achava que eles iriam fugir disso, não é? Eles deveriam ter nos esperado. #OpMegaupload
> Os seguintes sites foram atingidos em resposta ao bloqueio do megaupload.com pelo FBI :) Tango Down.[61]

O documento foi acompanhado por uma lista de sites mencionados no Pastebin em que o grupo afirma ter retirado como parte da operação; pelo menos nove sites da indústria do entretenimento e do governo foram confirmados como fora de serviço durante horas, incluindo as homepages do FBI e do Escritório de Copyright dos EUA, Recording Industry Association of America (RIAA) e da Motion Picture Association of America (MPAA). Também estão incluídos na demonstração informações pessoais do ex-senador e presidente da MPAA Chris Dodd e seus familiares. Após sequência de operações, em 20 de janeiro, o perfil de Twitter @AnonOps declarou a operação um sucesso, com mais de 5.635 pessoas que colaboraram com a ação através do software LOIC para derrubar os sites designados no ato.

Em consequência das operações orquestradas pelo Anonymous em Janeiro de 2012, a luta pelos privilégios do Megaupload é retomada pelo Partido Pirata espanhol, da Catalunha, ramificação do Partido Pirata Internacional, bem como o Partido Pirata do Reino Unido. O pressuposto foi que, enquanto o FBI pode ter justificado a penalização por violação de direitos autorais, o impacto do bloqueio foi consideravelmente absoluto, uma vez que muitos indivíduos e organizações tiveram seus arquivos e informações destruídas quando passaram a utilizar o serviço.

---

[61] O comunicado do Pastebin pode ser visto aqui http://pastebin.com/WEydcBVV. Acesso: 24 de Maio 2016.

> Independentemente da ideologia, ou opiniões sobre a legalidade ou a moralidade das pessoas que executam o Megaupload, ações como o encerramento deste serviço causará enormes danos para o utilizador legítimo local e são violações inaceitáveis e desproporcionais sobre os seus direitos e liberdade de informação na Internet.[62]

No final, o Partido Pirata da Catalunha conseguiu liderar a campanha com o apoio de vários partidos piratas pelo mundo e ainda dar espaço à indivíduos que quisessem se integrar ao movimento pirata. Visto assim, para Samuel (2014), a variedade de abordagens e agendas de ações da resistência na Internet também fornecem uma oportunidade para atuar em movimentos de hacktivismo no levante das questões: a capacidade do hacktivismo para corresponder com ações coletivas e desordenadas, é progressivamente a mais forte evidência para sua ampla relevância em ações políticas.

2.1.7 Operação Bahrain – 2012

Perante o cenário de milhares de manifestantes em demonstração a favor da democracia, liberdades civis e transparência na sociedade civil pelo mundo, a resistência ativista se espalha em Bahrain. Durante choque com a polícia entre ondas de gás lacrimogêneo e greves de fome, princípio que chamou a atenção da força tática da Internet: o Anonymous, mais uma vez. Em Abril de 2012, o evento automotivo da Fórmula 1, portanto, foi o palco principal de alerta ao reino de Bahrain que o país estaria sofrendo um distorcimento nos pilares básicos da democracia.

Em contexto histórico, o Bahrain Grand Prix foi o cenário para a reação violenta dos manifestantes após executivos e autoridades ridicularizarem a situação das desmonstrações pautada pela mídia internacional sobre a violência política no reino do Golfo Pérsico. "Uma quantidade de manifestantes e vândalos foram presos por participar de protestos ilegais e assembléias ao ar livre, durante bloqueio de estradas e ponto de tráfego de outros cidadãos, atacando-os com bombas de gás, barras de ferro e

---

[62] Anúncio da campanha do Partido Pirata Internacional contra as acusações do Megaupload, Janeiro de 2012. Ver em http://piratetimes.net/pirate-parties-help-victims-of-megaupload-siezure/. Acesso: 24 de Maio 2016.

pedras," diz a *Information Affairs Authority*[63] em comunicado, citando o major-general Tariq Al Hassan como compositor da credibilidade política do país.

No entanto, os manifestantes, juntamente com os ativistas e ONGs de direitos humanos, acusaram os governantes de Bahrain de usar o evento da Fórmula 1 para aperfeiçoar sua imagem internacional e culpar a minoria da população por ocasionar uma crise política e social. Na sequência do ataque inicial ao site oficial da Fórmula 1, o coletivo Anonymous começava por direcionar ataques de DdoS a servidores afiliados com o evento esportivo e excepcionalmente *home pages* do governo de Bahrain. Os ataques foram lançados como parte do projeto *Operation Bahrein,* assim como o coletivo hacker havia comunicado a Bernie Eccelstone, CEO da Fórmula 1, informando passo a passo sobre como seria feita a operação.

Logo após os primeiros ataques, o perfil mais popular do grupo Anonymous, YourAnonNews, relataram que haviam derrubado temporariamente um dos sites do departamento de defesa de Bahrain, juntamente com a FIA.com[64]. Em consequência da atuação autoritária do governo contra os cidadãos de Bahrain, o coletivo postou uma declaração sobre os competidores do site da Fórmula 1, condenando o regime do Rei Hamad bin Khalifa Al:

> "Por mais de um ano o povo de Bahrain têm lutado contra o regime opressivo do rei Hamad bin Khalifa Al", diz o comunicado. "Eles foram assassinados nas ruas, correr com os veículos, espancados, torturados, gás lacrimogéneo, sequestrado pela polícia, tiveram seus negócios vandalizados pela polícia, e têm bombas de gás lacrimogêneo atirado para suas casas em todas as noites."

[63] Formado em julho de 2010 por um decreto do Rei Hamad separando a agenda de informações a partir do que era então conhecido como o "Ministério da Cultura e Informação", a Autoridade de Assuntos de Informação refere-se ao Ministério da Informação de Bahrein.

[64] Site oficial da Federação Internacional do Automóvel; Associação Esportiva sediada em Genebra, na Suíça.
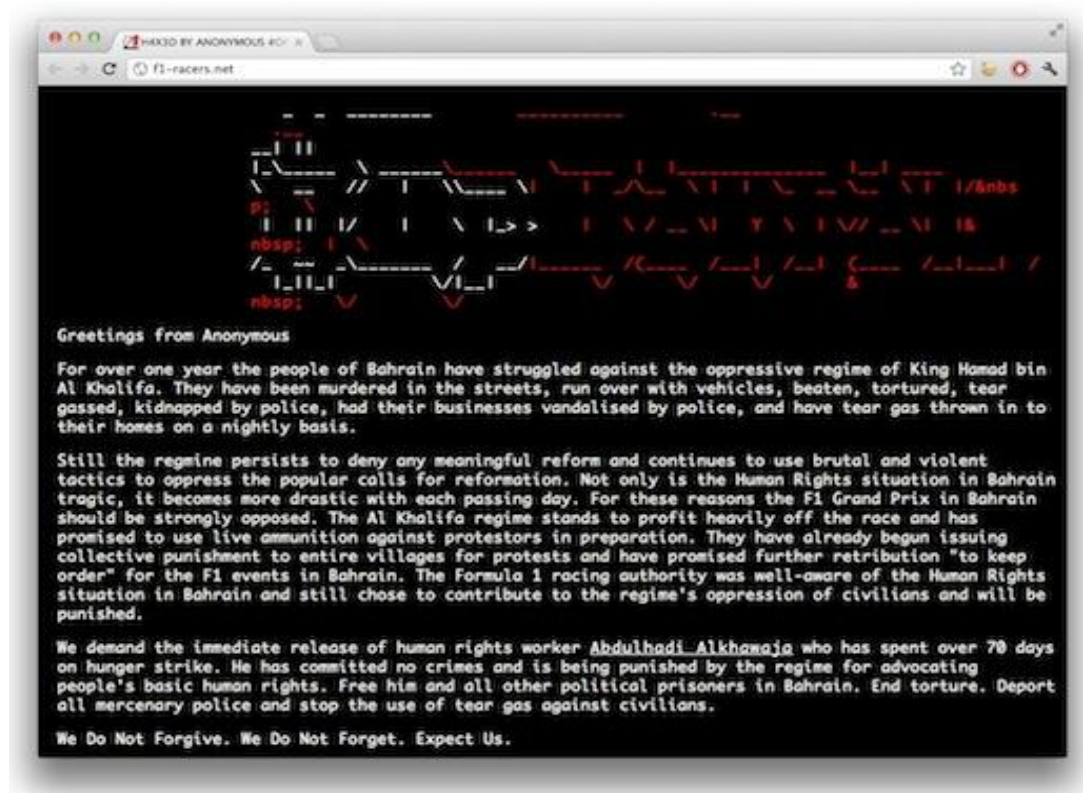
Figura 7: Mensagem fixada no site da FIA

Em tese, Samuel (2014) simplifica que a questão dos alvos de ações hacktivistas se tornam variadas como suas formas de implementação técnica e prática. Por isso, é discutível incluir um levantamento de alguns dos incidentes mais conhecidos de hacktivismo, tomando por base a Operação Bahrain, como uma evidência de que certos grupos e linhas de conflito são peculiares e aparecem com mais frequência nos cenários: guerras cibernéticas entre Índia e Paquistão, Israel e Palestina, China e EUA; hacktivismo anti-globalização; hacktivismo anti-cultural; hacktivismo social conservador; e contra a política interna dos EUA.

> Political cracking is conducted by hacktivists from hacker-programmer activism, and consists of forms of hacktivism that are consisten with what I call an “outlaw” orientation. There are the most illegal forms of hacktivismo such as defacements, redirects, denial of service attacks, sabotage, and information theft. (…) Finally, we have performative hacktivism, which is practiced by hacktivists from artist-activist backgrounds who have a transgressive orientation. Its forms are web site parodies and virtual sit-ins, most often as part of anti-corporate, anti-

> globalization, or pro-independence protests (Samuel, 2014, p.15).[65]

Nexte contexto, hackers realizam um novo modo de resistência que passa pelo conhecimento e pela autoformação de indivíduos autônomos e colaborativos (Amadeu, 2010). Na cena hacker do coletivo Anonymous, ações como a Operação Bahrain ocasionaram na eficiência de atividades simultâneas e eventuais por lugares onde princípios básicos de direitos humanos estariam ameaçados por autoridades governamentais. Ou seja, em contraponto, as operações superaram um eco universal em diferentes grupos alternativos de resistência digital pelo mundo.

Nas orientações da antropóloga Gabriella Coleman (2014), as ações de hacking do Anonymous são vistas como imparciais e politicamente desordenadas, o que provoca abalo entre ramificações de grupos de hackers pela Internet que anseiam por atenção midiática, especialmente pelo fato de que o Anonymous conseguiu conquistar a atenção da imprensa internacional sem se atentar à maneira de estarem expostos individualmente. Além de suas táticas tradicionais, o Anonymous também incluiu na lista de ações a “call bombing” – ou bombardeio de chamadas –, atingindo uma lista de números de telefones oficiais da Fórmula 1, bem como as táticas de envio de spam para os e-mails.

Enquanto Bahrain ainda testemunhava protestos por um ano, o reino do Golfo Pérsico foi incapaz de obter o mesmo apoio popular global que os seus vizinhos de fronteira como o Egito e Síria, os quais haviam conquistado a confiança dos cidadãos após a Primavera Árabe. Em troca da paralisação dos protestos, os cidadãos em ação com o coletivo do Anonymous solicitavam o cancelamento do Grand Prix, que foi abandonado em 2011, após semanas de demonstrações pelo país. A responsável pela organização da Fórmula 1, a FIA, decidiu manter o evento automobilístico, mesmo com o crescimento das tensões entre as forças de segurança e manifestantes.

[65]Tradução nossa: Hacking político é conduzido por hacktivistas programadores, o que consistem em formas de hacktivismo que eu chamo de uma orientação de "fora da lei". Existem formas mais ilegais de hacktivismo, tais como desfigurações, redirecionamentos, ataques de negação de serviço, sabotagem e roubo de informações. (...) Finalmente, temos o hacktivismo performativo, que é praticado por ativistas artísticos praticados pelos hacktivistas com uma orientação transgressiva. Suas formas mais comuns são paródias e manifestações pacíficas virtuais, na maioria das vezes como parte de um protesto anti-corporativo, anti-globalização, ou pró-independência.

2.1.8 Operação Israel – 2013

A Operação Israel, também conhecida como *#OpIsrael*, foi mais uma campanha de retaliação cibernética do grupo Anonymous, com o propósito básico de disseminar protestos em massa contra as ações militares da *Operation Pillar of Defense*[66] - que também incluíam ameaça à liberdade de informação na Internet - através de desconfiguração de sites do governo israelense por meio de DdoS, suporte em demonstrações públicas e vazamento de dados governamentais.

No início de novembro de 2012, as Forças de Defesa de Israel[67] conseguiu conduzir o momento para as redes sociais, em especial o Twitter, para uma atualização frequente sobre o status da guerra em Gaza. Como consequência, em 14 de novembro, o IDF assassinou Ahmed Jabari, chefe da base militar do Hamas, em um ataque aéreo. Sendo o comandante assassinado com mais prestígio do Hamas desde a guerra de Gaza de 2008, a notícia se difundiu pelos dois lados do mundo. “O IDF começou uma ampla campanha em sites ocultos de terroristas, sendo o principal alvo Hamas e Estado Islâmico”, diz porta-voz do IDF, em 14 de novembro de 2012.

Em 15 de novembro, em um comunicado no Twitter de um dos afiliados ao Anonymous, afirmou que o governo de Israel estaria ameaçando publicamente bloquear o acesso à Internet em Gaza. Como consequência, o coletivo decide apelar para ataques aos sites mais importantes do país. A publicação inclui um arquivo de "pacote de cuidados" nas versões em Inglês e Árabe contendo o comunicado de imprensa, instruções de primeiros socorros, um guia de proxy para esconder endereços de IP do usuário e um guia técnico sobre como contornar uma proibição de acesso à Internet.

No processo das atividades da derrubada dos servidores de Israel, o coletivo de hackers apresentou um conteúdo publicado no Pastebin[68], que possuia mais de 650

---

[66] Pilar Operação de Defesa foi uma força-tarefa militar de Israel, em operação por oito dias na Faixa de Gaza tomada pelo Hamas, que começou em 14 de Novembro de 2012, com a morte de Ahmed Jabari, chefe da base militar do Hamas. Ver em: http://www.globalsecurity.org/military/world/war/operation-pillar-of-defense.htm. Acesso: 25 de Maio de 2016.

[67] Israel Defense Forces (IDF) - http://www.idf.il.

[68] Sites desconfigurados: http://pastebin.com/Ms4nJSZx. Acesso em 24 de Maio 2016.

endereços de sites desfigurados, como parte da. Além disso, outro arquivo[69] de Pastebin foi criado para recolher informações úteis para os cidadãos de Gaza, incluindo links para os kits de primeiros socorros virtuais, como aplicativos de celulares, informações médicas, livestreams de protestos, links de notícias e tefones de organizações de direitos humanos, entre outros recursos. No mesmo dia, uma versão modificada do comunicado em forma de vídeo[70] foi postado no YouTube, em um perfil do Anonymous no Twitter e Facebook, lançados com a hashtag designada para o movimento: #OpIsrael.

Figura 8: No maior perfil do Anonymous, comunicava "Israel, todas as suas bases pertencem a nós"

Com a operação ainda em andamento, o Anonymous consegue expor informações pessoais de mais de 5.000 funcionários israelenses do Departamento de Defesa de Israel. No entanto, no dia seguinte, o link levava a uma página de ‘erro 404’. A ação foi do ministro das Finanças de Israel, Yuval Steinitz, após afirmar que o país havia bloqueado mais de 44 milhões de ataques cibernéticos em sites do governo para “evitar transtornos diplomáticos com outros países”. A repercussão da operação pela imprensa foi intimidadora para o coletivo de hackers. Sites de notícias que geralmente

[69] Conteúdo do Pastebin com ‘kit de primeiro-socorros’: http://pastebin.com/Yhy5e2ny. Acesso em 24 de Maio 2016.

[70] O vídeo release da Operação Israel pode ser visto aqui https://www.youtube.com/watch?v=PKrVYRu0oMY. Acesso em 26 de Maio 2016.

tratavam sobre cultura da internet e política internacional, como o Breitbart[71], Cnet[72], Forbes[73], Daily Dot[74], Vice[75] e Fox News[76], dirigiam-se ao grupo de hacktivistas de forma controversa em relação às suas ações.

Partindo do presuposto da Operação Israel, Samuel (2014) identifica o hacktivismo contemporâneo como uma forma progressista de se afirmar na subcultura da Internet, contexto que delimita transformações em culturas e comunidades alternativas pelo mundo, de forma subjacente. O dilema em representar uma guerrilha de hackers, como o Anonymous, na mídia tradicional é enfrentar uma represália de combinações de atos políticos que correspondem explicitamente com a computação e hacking.

No começo de Abril de 2013, dezenas de sites do governo israelense haviam sido derrubados, incluindo a Polícia de Israel, o Ministério da Defesa, Gabinete do Primeiro-Ministro, o Ministério de Imigrantes e do *Central Bureau of Statistics* – o escritório geral de coleta de dados do governo israelense. Em decorrência disso, o *Hackers News Bulletin*[77] compilou uma lista dos principais sites israelenses que foram desfigurados pelo DDoS e sobrecarga de ataques. Assim como Gabriella Coleman (2004) determina, o hacktivismo do Anonymous emerge em contextos de diferentes ideais culturais, sociais e políticos na sociedade da informação ao longo da perpetuação de comunidades alternativas cada vez mais descentralizadas, difundindo a ideia se desvencilhar de um controle autoritário na sociedade da informação centralizada.

[71] http://www.breitbart.com/big-government/2012/11/16/anonymous-launches-opisrael-in-retaliation-for-gaza-strikes/. Acesso em 24 de Maio de 2016

[72] http://www.cnet.com/news/anonymous-targets-israeli-web-sites-in-protest-over-gaza/. Acesso em 24 de Maio 2016.

[73]http://www.forbes.com/sites/andygreenberg/2012/11/19/anonymous-hackers-ramp-up-israeli-web-attacks-and-data-breaches-as-gaza-conflict-rages-2/#715251554573. Acesso em 24 de Maio 2016.

[74] http://www.dailydot.com/news/anonymous-opisrael-israel-attacks-anon-gaza/. Acesso em 24 de Maio de 2016.

[75] http://www.vice.com/read/the-gaza-strip-cyber-war. Acesso em 24 de Maio de 2016.

[76]http://www.foxnews.com/world/2012/11/19/hackers-target-israel-with-millions-attacks-as-hamas-rockets-continue-to-fall.html. Acesso em 24 de Maio de 2016.

[77] Site popular de segurança e computação - http://www.hackersnewsbulletin.com/.
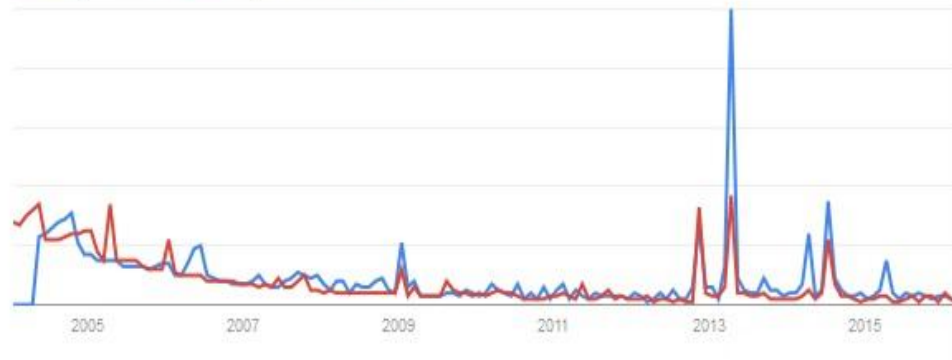
Figura 9: Estatística de popularidade da Operação Israel (Google Trends)

O Twitter principal da operação, a @OpIsrael estimou que as ações estavam em US $ 3 bilhões de dólares em danos consequentes de operações. Enquanto isso, o Anonymous e o grupo turco *RedHack*[78] teriam publicado informações pessoais de mais de 30.000 agentes israelenses, incluindo seus nomes, locais, números de telefone e endereços de e-mail, embora que ainda não esteja claro se os dados foram obtidos durante o último ataque da Operação Israel.

[78] O RedHack é um grupo de hackers radicais-extremistas da Turquia fundado em 1997. O grupo reivindicou o hacking de instituições do Conselho do Ensino Superior da Turquia, as forças policiais turcas, o Exército turco, Türk Telekom (empresa de telecomunicações), e a Organização Nacional de Inteligência, entre outros.

Figura 10: O Twitter oficial da operação menciona o dano de 3 bilhões de dólares sobre os ataques aos sites do governo de Israel.

2.1.9 Operação Ferguson – 2010

O coletivo do Anonymous se encontra em um momento peculiarmente conflagrado quanto à legitimação de suas ações na inexistência de um líder para o movimento depois do ocorrido com o hacker Sabu, do LulzSec, em 2011. A Operação Ferguson iniciou uma fase eloquente do hacktivismo do Anonymous. No entanto, é necessário desiludir quaisquer suspeitas de que a hiper-agressividade registra o limite e variedade de repertório de ações pelo Anonymous (Galloway, 2014). Quando o policial Darren Wilson atira em um adolescente desarmado chamado Michael Brown, em 9 de agosto de 2014, na cidade de Ferguson, Missouri, a resposta do subúrbio de St. Louis, com descendência afro-americana, foi a motivação de uma onda de protestos nas ruas e na comunidade digital, invocando movimentos sociais e políticos, nas peculiaridades da resistência racial que vem permeando pelos Estados Unidos.

Enquanto a história como um todo possui múltiplas facetas, estendidas ao longo de manifestações influenciadas por resposta policial desproporcional, a Operação Ferguson se concentra ainda mais com protestos sinérgicos catalisados em torno de eventos influenciados por tragédias locais, como a morte de outro adolescente negro, Vonderrit Myers Jr. em outubro de 2014. A raiva que emergia desses movimentos são vistos como vitais para movimentos sociais, contexto em que estimulou os cidadãos de

Ferguson na luta pela justiça, resistência e liberdade. Tal é a amplitude da insatisfação generalizada que permeia as discussões pelas mídias sociais e refletem estas qualidades, como efeito de atos que fluem para este novo meio de discussão pública, com o apoio de coletivos alternativos.[79]

> As described above, the Internet may allow social behavior to occur because individuals can revert to their social identity—the social group is internalized individually. This means, however, that people are thrown back on their understanding of the group, and the possible courses of action and their consequences. They can no longer rely on others' views or direct influence in deciding what, for example, the best course of action is. Thereby, the web is likely to accentuate the importance of cognitive calculations about social movement participation (Postmes e Brunsting, 2002, p.296).[80]

A principal razão por o grupo Anonymous se envolver nos protestos em Ferguson foi em ocorrência de um alerta por um artista de rap local, Tef Poe, que chamou por socorro no Twitter, de acordo com a especialista no hacktivismo do Anonymous, Gabriella Coleman (2014), e os membros do coletivo. Um dia depois da tragédia, através da Operação Ferguson, o Anonymous divulga um comunicado solicitando ao Congresso norte-americano para aprovar uma lei que definiria "normas nacionais e rigorosas para a conduta policial." O grupo também advertiu o governo e o departamento policial de Ferguson sobre ciberataques caso se os manifestantes fossem reprimidos, perseguidos ou prejudicados de qualquer forma.

> "Se você atacar os manifestantes, vamos atacar cada servidor e computador que vocês tiverem. Vamos hackear e liberar informações pessoais sobre cada um dos membros do Departamento de Polícia de Ferguson, assim como qualquer

---

[79] RAMBUKANNA, Nathan. From #RaceFail to #Ferguson: The Digital Intimacies of Race-Activist Hashtag Publics. The Fibreculture Journal. Wilfrid Laurier University, 2015. - http://twentysix.fibreculturejournal.org/fcj-194-from-racefail-to-ferguson-the-digital-intimacies-of-race-activist-hashtag-publics/. Acesso em 27 de Maio de 2016.

[80] Tradução nossa: Como descrito acima, a Internet pode permitir que o comportamento social ocorresse, pois os indivíduos podem reverter a sua identidade social – a identidade social é interiorizada individualmente. Isto significa, no entanto, que as pessoas se aplicam quanto à sua compreensão do grupo, e os possíveis cursos de ações e suas conseqüências. Eles não podem contar com a opinião de outros ou influência direta na decisão do que, por exemplo, qual seja o melhor curso de uma ação. Desse modo, a Internet é susceptível de acentuar a importância de cálculos cognitivas sobre a participação do movimento social.

> outra instituição de jurisdição que participa do abuso. Vamos aproveitar todas as suas bases de dados e servidores de e-mail e despejar os dados na Internet. Este é o único aviso."[81]

Em entrevista à *Times*[82], Coleman diz que não há apoio unânime dentro da comunidade hacker do Anonymous. "É um grande debate contencioso entre hackers que têm um ponto de vista autêntico quanto à liberdade de expressão, e outros são mais contextuais", diz Coleman. "Há também um debate dentro do próprio Anonymous onde muitos hackers que realmente fazem o trabalho de intrusão não são fãs de 'doxing[83]' por duas razões: a) é tecnicamente desinteressante e b) às vezes estes estão tentando ganhar acesso a esses sites para interromper serviços."

Por um lado, o grupo de hacktivistas do Anonymous conseguiram auxiliar na propagação da hashtag #OpFerguson pelo Twitter, e incentivar as ações das comunidades de ativismo da Internet. A ideia foi implantada logo após a notícia sobre os eventos em toda a mídia convencional, impulsionando a hashtag como um dos assuntos mais comentados do ano de 2014, com 4000 acessos em apenas nove horas. Por outro lado, as escalas globais desses eventos expressam o surgimento de novos paradigmas ideológicos, o que poderá, eventualmente, trazer uma mudança política através de coletivismo online e offline (Grammatikopoulou, 2014).

Esta também não é a única hashtag de ativismo racial que surgiu a partir de eventos em mídias sociais. Outros, como #FergusonOctober, #IAmMichaelBrown e #BlackLivesMatter, destacam a ocorrência repetitiva de policiais brancos que atiram em adolescentes negros nos EUA. Para tanto, é certo mencionar que o coletivo estaria fragmentado; hackers que estariam auxiliando nos protestos da #OpFerguson; outros que não concordavam com a ideia de promover a ação devido à dispersão do coletivo

---

[81] Comunicado do Anonymous à Polícia de Ferguson, publicado em Pastebin: http://pastebin.com/KpmJKU8D. Acesso em 27 de Maio de 2016.

[82] Menções de Gabriella Coleman sobre as ações do Anonymous na Operação Ferguson, em artigo da Times: "What Anonymous Is Doing in Ferguson? - Ver em: http://time.com/3148925/ferguson-michael-brown-anonymous/. Acesso em 27 de Maio de 2016.

[83] Doxing é o processo de recuperação, hacking e publicação de informações de outras pessoas, tais como nomes, endereços, números de telefone e detalhes de cartão de crédito. Doxing pode ser direcionada a uma pessoa específica ou uma organização. Há muitas razões para doxing, mas um dos mais populares é o constrangimento. Doxing tambem é uma gíria que é derivada da palavra ".doc" pois documentos são muitas vezes recuperados e compartilhados. Hackers têm desenvolvido maneiras diferentes de DOX, mas um dos métodos mais comuns é hackear o e-mail da vítima. Uma vez que o e-mail tenha sido obtida, o hacker trabalha para descobrir a senha e abrir a conta da vítima para obter mais informações pessoais.

para fins divergentes do movimento hacker; uma minoria que se sentia indiferente em aplaudir ou auxiliar o ato.

> This is another interesting thing about Anonymous: It attracts those with some pretty deep technical skills to those with no technical skills -- one can find a place and a home with Anonymous. Historically, and with Ferguson and OpBART and even LulzSec, many of the hacks were not rocket science, as I like to say -- it's more a reflection of the sorry state of security on the Web. That said, definitely a handful of people like Jeremy Hammond and Mustafa Al-Bassam are really, bright hackers -- extremely bright. That's, I think, the interesting thing about Anonymous -- you definitely don't need people with deep, deep skills (Coleman, 2014).[84]

Em decorrência dos protestos, o espaço conquistador pelos ativistas em Ferguson foi cada vez mais ameaçado por violência policial e abuso de autoridades. Como parte do auxílio dos atos em Ferguson, o coletivo disponibiliza[85] aos ativistas um guia de sobrevivência, contendo passo a passo de autodefesa, utilização de máscaras de gás, se movimentar pelas ruas na presença de um grupo ou multidão para evitar detenções isoladas, entre outras utilidades de resistência urbana.

Na verdade, é importante ressaltar que estamos lidando aqui com diversas tendências políticas, algumas delas já formadas através dos movimentos sociais e políticos do passado e alguns que só começaram recentemente a tomar forma, como consequência dos novos cenários introduzidos pelo despertar das comunidades alternativas da Internet na utilização em massa das tecnologias de informação.

---

[84] Tradução nossa: Esta é outra coisa interessante sobre o Anonymous: eles atraem as pessoas com algumas habilidades técnicas muito profundas para quem não tem habilidades técnicas - pode-se encontrar um lugar e uma casa com Anonymous. Historicamente, and com Ferguson e a OpBART e até mesmo o LulzSec, muitos dos hacks não eram especialistas, como gosto de dizer - é mais um reflexo do estado lastimável da segurança na Web. Dito isto, definitivamente um punhado de pessoas como Jeremy Hammond e Mustafa Al-Bassam são hackers realmente brilhantes - extremamente brilhantes. Isso é, penso eu, a coisa mais interessante sobre o Anonymous - você definitivamente não precisa de pessoas com profundas habilidades.. Entrevista ao Washington Post, em 15 de Agosto de 2014. Ver em https://www.washingtonpost.com/news/the-switch/wp/2014/08/15/the-complete-guide-to-anonymous-and-opferguson/. Acesso em 28 de Maio de 2016.

[85] Todo o material e conteúdo da Operação Ferguson estão disponíveis na íntegra pelo site http://www.operationferguson.cf/.
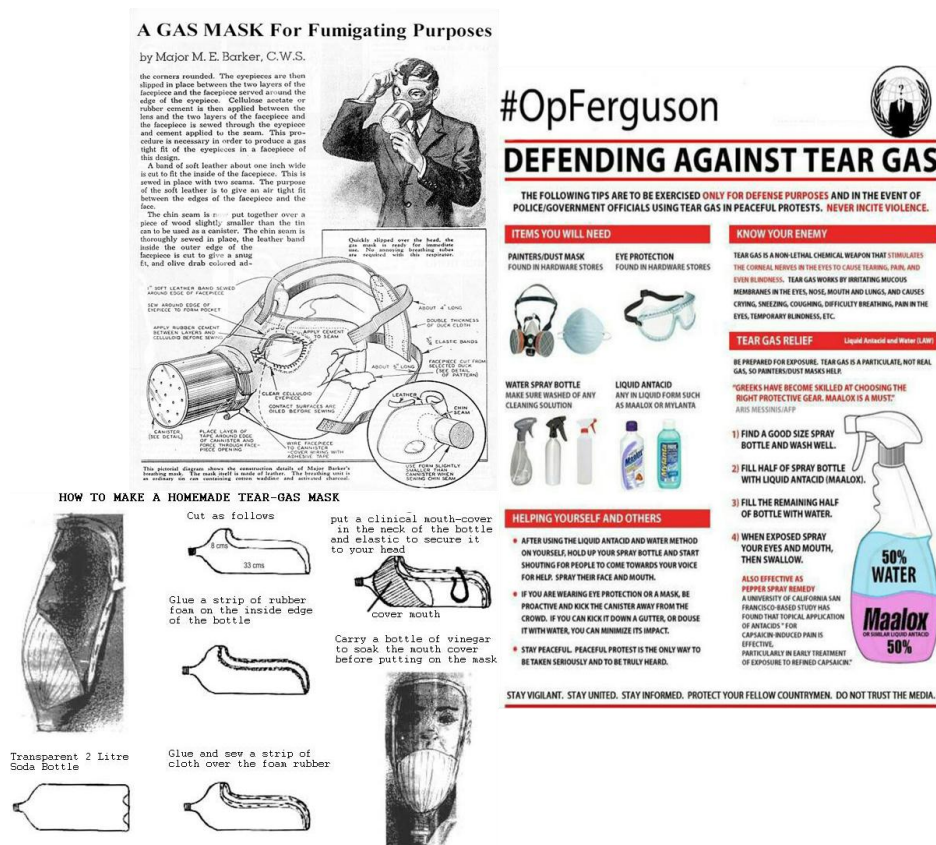
Figura 11: Folders disponíveis no kit de sobrevivência, elaborado pelo Anonymous

2.1.10 Operação ISIS - 2015

Uma característica importante das ações dos hackers do Anonymous é a capacidade do hacktivismo na atuação de várias ramificações ao mesmo tempo: ao contrário da maioria das formas de ação política, que exigem certo grau de cooperação em massa, a conduta de ciberguerrilha do Anonymous cria estímulos em conflitos internos de ação espontânea.

A operação contra a propaganda em massa do Estado Islâmico (Islamic State of Iraq) foi anunciada pela primeira vez em 21 de junho de 2014, desginada pelo nome de *Operação NO2ISIS*, pouco depois que um perfil de Twitter do coletivo, @TheAnonMessage foi hackeado e comprometido por membros do ISIS com imagens de violência. A operação inicialmente procurou derrubar sites do governo de, pelo menos, três países que têm sido suspeitos de financiamento ou de apoio ao grupo

terrorista. Porém, o escopo da missão foi ampliada como esfera de influência do ISIS ao continuar a crescer pelo Oriente Médio, bem como a sua presença na Internet.
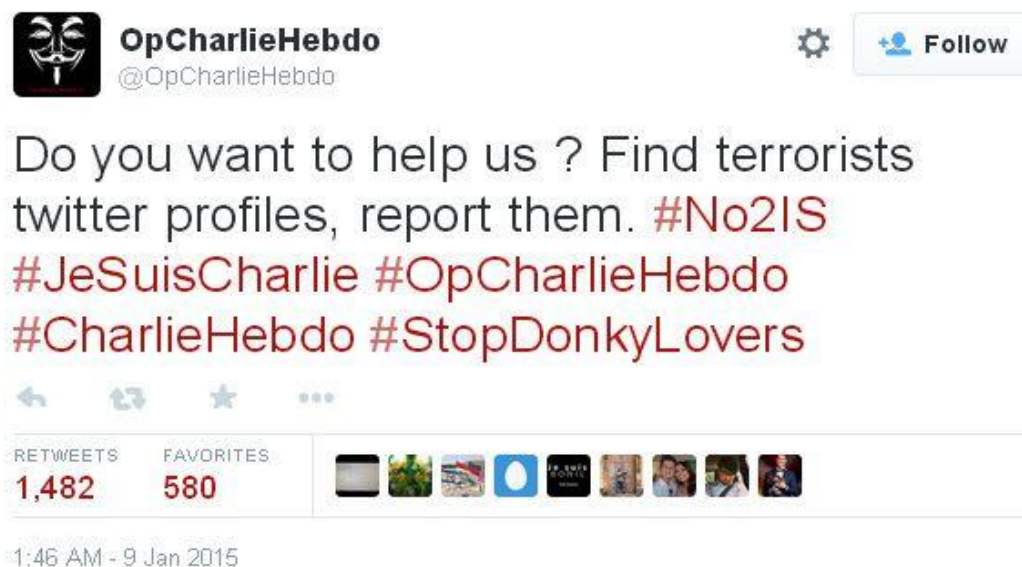
Figura 12: "Querem nos ajudar? Encontre perfis de terroristas no twitter, denunciem", publicou OpCharlieHebdo

No início de Janeiro de 2015, a guerra do Anonymous contra o ISIS tomou um rumo importante com o lançamento da #OpCharlieHebdo no cenário dos ataques terroristas contra a sede da revista satírica francesa em Paris Charlie Hebdo, que resultou na morte de escritores, cartunistas e policiais.

> OpISIS is a multi-faceted operation which has ebbed and flowed over time, although its most public triumphs have come in that most public of arenas, social media. There are hacking, DDoS, and other components to it as well. It is one of the rare instances where the US Government does not appear to be exerting any force to oppose an Anonymous Operation, because with the current state of US government cyberwar capacity, leaving it to Anonymous allows them to allocate their still-limited resources more strategically than playing whack-a-mole with ISIS on Twitter and Facebook and pointing botnets at tangential sites.[86]

[86] Resposta do hacker e ex-membro do Anonymous KarmaCop, através de email, em 5 de Março de 2016. Tradução nossa: OpISIS é uma operação com múltiplas facetas de várias reviravoltas ao longo do tempo, apesar de seus maiores triunfos se tornaram mais públicos, pelas redes sociais. Houve hacking, DDoS, e outros componentes. É um dos raros casos em que o governo dos EUA não exerciam qualquer força para

Em 8 de fevereiro de 2015, o Anonymous publicou um vídeo no YouTube a fim de anunciar uma nova onda de ataques cibernéticos que envolviam invasão de sites, e-mail, perfis listados de Facebook e Twitter usados por membros do ISIS para recrutamento de novos terroristas. O conteúdo destaca que o coletivo Anonymous "é um grupo extremamente vasto, cujos membros vêm de uma variedade de origens sociais, religiosas e raciais, prontos para caçar o Estado Islâmico[87]."

Logo após anunciar a sequência de operações, o Anonymous afirmou ter desativado com êxito mais de 80 contas de Twitter afiliados ao Estado Islâmico. No terceiro dia na operação, o grupo conseguiu derrubar mais de 1.000 sites, 800 contas do Twitter[88], milhares de páginas do Facebook e 50 contas de e-mail suspeitas de serem executados por membros do ISIS, de acordo com uma lista publicada pela grupo através Pastebin[89]. O resultado do ataque do coletivo Anonymous rapidamente se espalhou por meio dos principais meios de comunicação, mas sua legitimidade era ostensivamente questionada.

---

se opor a uma operação do Anonymous, pois com o estado atual da capacidade de guerra cibernética do governo dos Estados Unidos, permitiram que o Anonymous usassem seus recursos, ainda que estrategicamente limitados para enfrentar o ISIS no Twitter e Facebook, apontando *botnets* em locais tangenciais.

[87] #OpISIS Continues - https://www.youtube.com/watch?v=BPE_sRhZp6M. Acesso em 29 de Maio 2016.

[88] Operation Isis: Anonymous takes down Twitter and Facebook accounts associated with extremist group - http://www.independent.co.uk/life-style/gadgets-and-tech/operation-isis-anonymous-vows-to-take-down-accounts-and-associated-with-extremist-group-10035199.html. Acesso em 30 de Maio 2016.

[89] Lista de perfis: http://pastebin.com/d8ND4rvV.

```
154. https://twitter.com/mhiisni          https://twitter.com/intent/user?user_id=393440365    342 K   TARGET N° 1 !!!
155. https://twitter.com/EYADQUNAIBI      https://twitter.com/intent/user?user_id=532700952    156 K followers
156. https://twitter.com/s_2017_          https://twitter.com/intent/user?user_id=241640145    116 K followers
157. https://twitter.com/zahran1970       https://twitter.com/intent/user?user_id=870434053    111 K followers
158. https://twitter.com/ZaidZamanHamid   https://twitter.com/intent/user?user_id=126966274    104 K followers
159. https://twitter.com/Al_forqaan       https://twitter.com/intent/user?user_id=399730349    88.1 K FOLLOWERS
160. https://twitter.com/IslamArmy01      https://twitter.com/intent/user?user_id=707052698    73700 followers
161. https://twitter.com/dralgzouli       https://twitter.com/intent/user?user_id=571854743    >>> 50,9 K Followers !!!
162. https://twitter.com/alheetari        https://twitter.com/intent/user?user_id=1100821141   47.900 followers (prédicateur)
163. https://twitter.com/Q8__HACK         https://twitter.com/intent/user?user_id=1249204051   37.000 followers
164. https://twitter.com/taweel_ruaa      https://twitter.com/intent/user?user_id=2534504508   30.000 folowers
165. https://twitter.com/salah_news3      https://twitter.com/intent/user?user_id=2901960090   26.100 followers
166. https://twitter.com/anjemchoudary    https://twitter.com/intent/user?user_id=263428605    26.000 followers << !!
167. https://twitter.com/Nsaaeet          https://twitter.com/intent/user?user_id=525504379    25600 followers
168. https://twitter.com/Latest111        https://twitter.com/intent/user?user_id=2813747288   24.4 K followers !
169. https://twitter.com/awsfasfasisis    https://twitter.com/intent/user?user_id=2807440143   23.3k folloers
170. https://twitter.com/motlaqghazai     https://twitter.com/intent/user?user_id=425726100    (22500 followers)
171. https://twitter.com/mri45555         https://twitter.com/intent/user?user_id=2684467195   20.500 followers
172. https://twitter.com/Abu_Baraa1       https://twitter.com/intent/user?user_id=513116847    20,000 follower
173. https://twitter.com/MohammadHlabi80  https://twitter.com/intent/user?user_id=2427673497   17,9 K followers
174. https://twitter.com/aman12000        https://twitter.com/intent/user?user_id=2835577020   17.600 followers
175. https://twitter.com/mamoonhatem      https://twitter.com/intent/user?user_id=2911174142   15,300 followers
176. https://twitter.com/thabet207        https://twitter.com/intent/user?user_id=619362308    15 K followers also has another
account
177. https://twitter.com/thabet209        https://twitter.com/intent/user?user_id=1510978010   (only 1943 followers)
178. https://twitter.com/soor18957        https://twitter.com/intent/user?user_id=2841241388   14.400 followers
179. https://twitter.com/fallujaty2       https://twitter.com/intent/user?user_id=2834912653   12.8 K followers !
180. https://twitter.com/ah_bawade        https://twitter.com/intent/user?user_id=2836021826   12.8 K FOLLOWERS
```

Figura 13: Lista de perfis de Twitter do Estado Islâmico que foram hackeadas

Por mais explosivo que o Anonymous ainda seja, a sua permanência na cena hacker como uma comunidade organizada e ao mesmo tempo, descentralizada, certamente não durou por muito tempo. O coletivo é atormentado por disputas internas, fragmentação, bem como pelo esgotamento de sua marca (Coleman, p.71, 2012). Nessa perspectiva, às vezes, os membros do coletivo, para desorientar os veículos de comunicação, propagam informações falsas de forma proposital sobre suas atividades. Tal finalidade é incorporada como uma tática de autodefesa, em alguns casos, e em outros casos, buscam persuadir as principais manchetes da imprensa internacional o que pode ser cativado pelas habilidades de hacking desconhecidas pelas entidades midiáticas.

O AntiSec[90], visto como um grupo de hackers formidáveis e afiliados com o Anonymous, puderam reivindicar a cena do hacktivismo nas proporções de um coletivo determinado em se desviar dos tablóides e manchetes de jornais. Os hackers, por vezes, dependem dos botnets - redes de computadores comprometidos - para manter

[90] É um movimento de oposição a indústria de segurança de computadores. AntiSec é contra a divulgação completa de informações relacionadas limitado a: vulnerabilidades de software, exploits, técnicas de exploração, ferramentas de hacking, atacando públicos de redes sociais e pontos de distribuição dessa informação. Ver em: http://www.bbc.com/news/technology-17548704. Acesso em 31 de Maio 2016.

momentaneamente um site offline, sem a necessidade de anunciar o ocorrido na imprensa.

> Its real threat may lie not so much in its ability to organise cyberattacks but in the way it has become a beacon, a unified front against censorship and surveillance. It might be best thought of as the irascible and provocative protest wing of the internet's nascent free speech and privacy movement. Though it works to publicise specific issues at the most inconvenient time for the individual, group or company being exposed, it also brings into sharp focus an important trend, dramatising the value of privacy and anonymity in an era where both are rapidly eroding. Anonymous, of course, champions anonymity, and this is echoed in both the iconography associated with it and its ethical codes (Coleman, 2012, p.70).[91]

Desde então, o método de protestos do coletivo passou por transformações cada vez mais operacionais com intenção vingativa do que por consciência política. Em 14 de novembro de 2015, o Anonymous envia um mensagem em vídeo declarando guerra contra o ISIS em resposta aos ataques em Paris, em 13 de novembro, fato que deixou mais de 120 mortos. No vídeo[92], um membro narra em francês sobre a intenção do grupo hacker em 'caçar' o Estado Islâmico.

> You should know that we will find you and we will not let you go. Expect massive cyber attacks. War is declared. Get prepared. The French people are stronger than you and will come out of this atrocity even stronger.[93]

[91] Tradução nossa: Sua ameaça real pode estar não tanto na sua capacidade para organizar ataques cibernéticos mas na forma como ele se tornou um farol, uma frente unificada contra a censura e vigilância. Poderia ser melhor pensado como o irascível e provocante protestar ala do movimento de expressão e privacidade livre nascente da internet. Embora ele funciona para divulgar questões específicas no momento mais inconveniente para o indivíduo, grupo ou empresa que está sendo exposto, mas também traz em afiada concentrar uma tendência importante, dramatizando o valor da privacidade e anonimato em uma época em que ambos estão erodindo rapidamente. Anonymous, é claro, campeões o anonimato, e isso é ecoado tanto na iconografia associada a ele e seus códigos de ética.

[92] O pronunciamento do Anonymous ao Estado Islâmico pode ser visto aqui https://www.youtube.com/watch?v=RwGGcZoRs-k. Acesso 31 de Maio 2016.

[93] Uma parte da mensagem publicada em vídeo, do Anonymous. Tradução nossa: Você deve saber que iremos encontrá-los e não vamos deixar vocês irem. Espere por ataques cibernéticos em massa. A guerra está declarada. Se prepare. Os franceses são mais fortes do que vocês e irão sair dessa atrocidade ainda mais fortes.

Com base na hashtag *#OpParis*, a mais recente onda de esforços do Anonymous contra o Estado islâmico foi anunciada juntamento pelo perfil afiliado do grupo, *@GroupAnon*, um dos elos principais de relações públicas digitais do coletivo, bem como o recém-criado Twitter *@OpParis*. Nos dias seguintes, milhares de perfis de Twitter pró-ISIS foram derrubadas pelo grupo até então.

Figura 14: @GroupAnon anuncia que o Anonymous "está em guerra com Daesh" e que "não irão parar de se opor ao Estado Islâmico". Na @opparisofficial, afirmam que mais de 5.500 perfis associados com o Estado islâmico foram hackeadas

A partir do momento em que a Operação Israel recebe visibilidade pela imprensa e plataformas midiáticas, as ações fizeram com que uma minoria desinteressada na operação participasse de eventos lúdicos como protestos alternativos. Em 3 de dezembro de 2015, um arquivo de texto foi enviado em Ghostbin[94] anunciando que os

[94] Campanha do Troll ISIS Day, publicado em Ghostbin: https://ghostbin.com/paste/ucsf3.

responsáveis pela Operação ISIS planejaram o "Troll ISIS Day", a qual os hackers, juntamente com outros usuários pelas redes sociais compartilhariam a brincadeira pela Internet contra perfis de apoio ao ISIS, utilizando as hashtags #Daesh e #Daeshbags, sendo que ambos são rótulos depreciativos para a organização.

> […] on December 11th we will show them that we are not afraid, we will not just hide in our fear, we are the majority and with our strength in numbers we can make a real difference. We will mock them for the idiots they are. We will show them what they really are they do not stand for a religion, they do not stand for a god, they are brainwashers teaching from the young to the old their propaganda against the 'west' when in reality they are just increasing the distance between countries by giving many a bad name.[95]
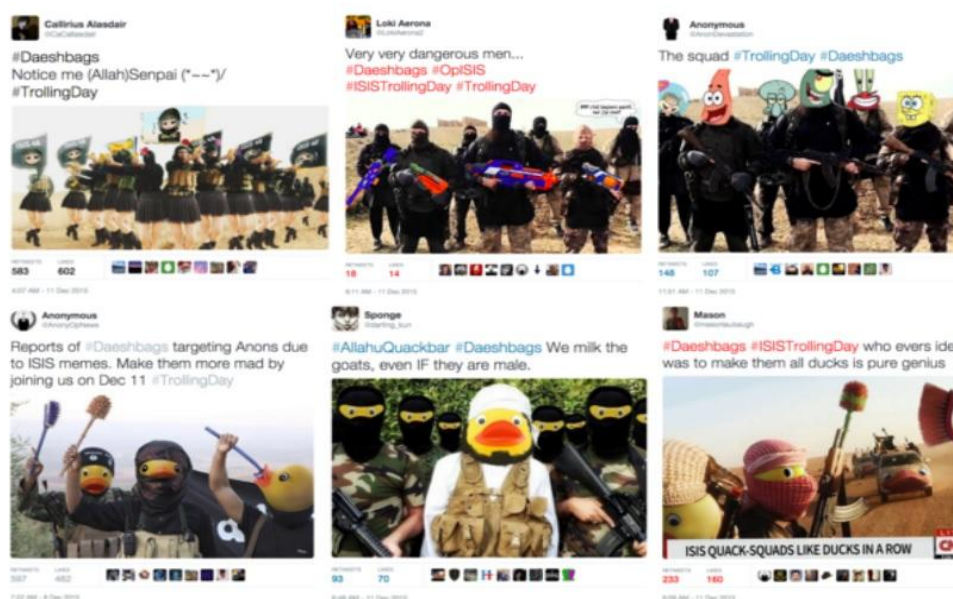
Figura 15: O coletivo conseguiu manifestar toda a comunidade virtual de redes sociais com imagens cômicas ridicularizando o Estado Islâmico

[95] Tradução nossa: Em 11 de dezembro vamos mostrar a eles que não temos medo, não vamos simplesmente nos esconder em nosso medo, nós somos maioria e com a nossa força em números, podemos fazer uma grande diferença. Nós vamos zombá-los o quão idiotas são. Vamos mostrar-lhes o que eles realmente são e que não representam uma religião, não representam um deus, fazem lavagem cerebral em jovens contra o "Ocidente", quando na realidade eles estão apenas aumentando a distância entre os países, dando a muitos um nome ruim. Mensagem do Anonymous sobre o "ISIS Trolling Day", disponível em https://ghostbin.com/paste/ucsf3. Acesso: 29 de Maio 2016.

Nos dias seguintes, sites de notícias do *IbTime*[96]*s* e *Express*[97] relaram que uma série de manifestações coordenadas contra o ISIS seriam realizados em 11 de dezembro nas principais cidades ao redor do mundo, incluindo Los Angeles, Nova York, Seattle, México City, Vancouver, Paris, Madrid e Cannes, entre muitos outros. Em 11 de dezembro, uma multidão no Twitter começou a compartilhar uma quantidade extraordinária de imagens em paródias ridicularizando o desempenho do ISIS, ao utiliarem as hashtags predeterminadas (#Daesh e #Daeshbags), bem como uma sequencia de hacking de uma lista de palavras-chave árabe, frases e hashtags com o objetivo de propagar um contra-ataque ironico contra a propaganda do Estado Islamico na Internet.

2.2 OPERAÇÃO ESTADO ISLÂMICO E A GUERRA DA INFORMAÇÃO

Embora muitos Anons ainda seguiam uma ideia ciberanárquica, seus métodos consistiam na propagação de informações sobre o movimento pela mídia global na busca pela reputação em nome de operações como o Projeto Chanology, Operação Primavera Àrabe, Operação PayBack, Operação BART, Operação HBGary e Operação ISIS. Houve momentos em que o lançamento de ações como estas fundamentava-se em apenas proteger a liberdade de expressão em várias partes pelo mundo (Coleman, 2012).

Enquanto os hackers dos anos 1960 podem não ter vencido a batalha da informação livre, estes conseguiram esclarecer o lado ambíguo do controle social na Internet, o que consequentemente foi mais resistente entre a década de 80 e 90, quando ciberataques eram comumente vistos como ciberterrorismo (McLaughlin, 2012). O último aspecto que realmente faz o Anonymous um desafio para os veículos de mídia hoje e que os tornam impossíveis de distinguir entre hacktivismo, vigilantismo e ações coletivas é que na internet, os fluxos de informação são indistintos.

[96] Anonymous Plans To Troll ISIS On Twitter, Facebook, Instagram And YouTube - http://www.ibtimes.com/anonymous-plans-troll-isis-twitter-facebook-instagram-youtube-2213992. Acesso em 30 de Maio de 2016.

[97] Hackers Anonymous will TROLL Islamic State in day of defiance against evil jihadist - http://www.express.co.uk/news/world/624951/Anonymous-troll-ISIS-December-11. Acesso em 30 de Maio 2016.

> Traditionally, many journalists have sensationalized representations of geeks and hackers by portraying them as malicious teenage boys, dwelling in their parents' basement and raising Internet hell as they channel anger stemming from psychological isolation. Nor is the significance of geek and hacker action accurately captured by one of the most prevalent sets of tropes currently used by academics and journalists to describe the digital present: the existence of a so-called digital generation or of digital natives whose sense of self and whose ethical frames are said to derive from their common use of social media technologies, like Facebook and Twitter, and digital devices, like cell phones (Coleman, 2012, p. 512).[98]

Mesmo que ainda existam diretrizes pelos quais se distinguem entre diferentes formas de ação política, é importante sinalizar aqui o papel político dos atores tecnológicos, tais como aqueles envolvidos nas operações do Anonymous durante as retaliações contra as forças do Estado Islâmico na Internet. Muitos hackers geralmente se envolvem em esforços para aumentar a participação na comunidade virtual. Sendo assim, o exemplo do Anonymous é o mais instrutivo quando analisamos sua participação de um grupo de hackers que se perpetuou na Internet como ciber-revolucionários pela imprensa, durante as ações da Operação ISIS, entre o final de 2014 e começo de 2016.

No site da revista *Foreign Policy*[99], o jornalista Emerson Brooking publicou em Novembro de 2015, um artigo dedicado à trama de distinções operativas entre o grupo Anonymous e o Estado Islâmico, como abordagens diferentes quando se trata de ciberterrorismo, pois se levar em conta a conduta dos hackers Anonymous, sua cultura prevalace ainda que fragmentada. Brooking descreve que “na luta contra o Estado islâmico, o coletivo de hackers se encontrava dividido por uma crise existencial”.

Porém, o que exatamente significa quando um grupo formado para desrespeitar as autoridades, se encontra em um conflito cibernético com os mesmos objetivos que o

---

[98] Tradução nossa: Tradicionalmente, muitos jornalistas têm representações sensacionalistas de geeks e hackers ao retratá-los como adolescentes mal-intencionados, morando no porão da casa de seus pais e trazendo o inferno à Internet assim como eles canalizam a raiva decorrente do isolamento psicológico. Nem é o significado da ação geek e hacker delimitadas de modo exato por um dos conjuntos mais prevalentes de contextos atualmente utilizados por acadêmicos e jornalistas para descrever o presente digital: a existência de uma chamada geração digital ou de nativos digitais os quais cenários e sensos éticos são para derivar da sua utilização comum de tecnologias de mídia social, como Facebook e Twitter, e dispositivos digitais, como telefones celulares.

[99] Anonymous Vs. Estado Islâmico: http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/. Acesso em 31 de Maio 2016.

governo dos EUA? Em debates públicos e privados, membros do Anonymous vêm lutando pelo passado do grupo com um presente incerto. Embora alguns membros do Estado Islâmico neguem a ligação com os hacktivistas, a distinção é mais lúcida entre ambos, contexto em que os veículos de comunicação se deparam com dificuldades em configurar as informações deste cenário para o público.

A diferença da *#OpISIS* com outras operações já realizadas pelo Anonymous é que esta é vista como uma ação ostensivamente plana e sem liderança, ainda que algumas delas sejam sustentadas por dezenas de membros que uma vez estiveram presentes em momentos históricos do hacktivismo, a fim de sustentar o núcleo do movimento. De acordo com Jordan e Taylor (1998), grupos fragmentados de hackers tendem assim a se concentrar em atos diferentes, como derrubar sites, localizar contas de Twitter e vídeos de propaganda do Estado Islâmico, infiltração em fóruns jihadistas, sendo que suas funções acabam por ser convergentes e divergentes de forma aleatória. O resultado é orgânico e caótico.

Figura 16: Um membro do grupo associado ao Anonymous faz uma declaração em imagem estática de um vídeo divulgado em 16 de novembro de 2015[100] (Foto: Reuters)

[100] Vídeo do Anonymous que anuncia guerra contra o Estado Islâmico na Internet. Ver em https://www.youtube.com/watch?v=BAUZnDIWu2I. Acesso em 29 de Maio 2016.

Em entrevista para a CBS News em Novembro de 2015[101], Gabriella Coleman sugeriu que, agora, para muitas pessoas que aderiram à causa do movimento Anonymous, a criação de uma rede imensa de hackers e ativistas com os esforços em atingir o Estado Islâmico se mantém em uma posição anárquica na história da Internet. "O Anonymous inicialmente era composto por uma tripulação menor, basicamente, para estabelecer um controle de qualidade da operação", disse Coleman. “Você observa o que está acontecendo com toda essa interação atual - das operações do Anonymous - e verá que não há muito efeito, e não tem nada a ver com o próprio movimento do Anonymous, de fato, se adequa mais com o cenário de que o Estado Islâmico garantiu a atenção da mídia mundial em tantos outros canais de comunicação, porém a #OpISIS assumiu uma posição melhor quanto à operação #OpParis, pois estavam agindo por muito mais tempo e com uma equipe menor de pessoas”, concluiu.

> ISIS is small state that brutally censors visiting journalists and its own people. As such it must be opposed. The question is in what manner it should be opposed. We think it's great if people want to hack ISIS and publish their secrets. But engaging in social media censorship campaigns and dealing with intelligence contractors and government agents, is deeply stupid. The former will contribute to legitimize the spread of internet censorship and will lead to the increased censorship for everyone, including Anonymous. Dealing with government agents et al will not only result in many more informers in Anonymous bu twill also damage its reputation as it will lead to a view that Anonymous is too close to US intelligence interests. The same intelligence industry that runs their own NSA hacker operations against ISIS uses the same counter-terrorism justification to spy on everyday civilians with no regards for rights to privacy, encryption, or anonymity. They have always targeted Anonymous and other dissident groups as terrorists, and when they aren’t trying to discredit or imprison us, they are attempting to co-opt us – sometimes openly by attending conferences like DEFCON, seducing us with promises of money or calls for patriotic duty, other times covertly lurking around IRC channels attempting to steer us unwittingly into supporting their agenda. We would like to strongly advise - while we cannot speak for the whole of Anonymous - to always release information to the public, as we want to operate in its interest. Any attempts to act in secrecy, supporting political or governmental organizations, will be discouraged by us or completely ignored to safeguard our allies and supporters fighting for openness and transparency within governments,

[101] ‘Anonymous vs. ISIS: Who has the upper hand in social media war?’ http://www.cbsnews.com/news/anonymous-vs-isis-social-media-war/. Acesso em 01 de Junho 2016.

> dictatorships and organizations around the globe that control various aspects of our lives. We are on the side of the oppressed, not the oppressors. We support the victims of war, not the war-makers. [102]

A cobertura da mídia sobre o ativismo virtual tem se concentrado principalmente, se não exclusivamente, no papel da Internet em incidentes dignos de serem publicados e por apresentarem pontos críticos jornalísticos. A imprensa atua em coberturas sobre invasões e ataques cibernéticos muito proeminente quando estas práticas se deflagram contra aspectos do cotidiano de um público ou indivíduo. (Postmes e Brunsting, p. 292, 2002). Por exemplo, os ataques que causaram o desligamento dos servidores da Casa Branca, em Maio de 1999[103], contribuiu para que as manchetes dos grandes veículos de comunicação espalhassem o fato por toda a mídia de massa.

Da mesma forma, as atividades dos hackers têm consistentemente atraído a atenção dos meios de comunicação, erodindo do público a confiança no comércio electrônico e da Internet em geral. Mais uma vez, é importante ressaltar que muitos

---

[102] Tradução nossa: ISIS é um pequeno estado que brutalmente censura jornalistas visitantes e seu próprio povo. Como tal, deve ser combatida. A questão é de que maneira isso deve ser combatido. Nós achamos que é se as pessoas querem hackear o ISIS e publicar seus segredos. Mas se engajar em campanhas de censura pelas mídia sociais e lidar com agências de inteligência e agentes do governo, é profundamente estúpido. Essa será uma contribuição para legitimar a propagação da censura na internet e levará ao aumento da censura para todos, incluindo o Anonymous. Lidar com agentes do governo etc e tal não só irá resultar em mais informantes como Anonymous também à danos a sua reputação como ponto de vista que o Anonymous é próximo quanto aos interesses da inteligência dos EUA. O mesmo setor de inteligência que executa as suas próprias operações de hackers da NSA contra o ISIS usa a mesma justificativa de combate ao terrorismo para espionar civis todo dia, sem dizer respeito aos direitos à privacidade, criptografia ou anonimato. Essas agências sempre interceptaram o Anonymous e outros grupos dissidentes como terroristas, e quando eles não estão tentando desonrar ou aprisionar-nos, eles tantam nos cooptar - às vezes abertamente, participando de conferências como a DEFCON, nos seduzindo com promessas de dinheiro ou de chamadas para o dever patriótico, outras vezes secretamente rondando canais de IRC que tentam nos orientar involuntariamente em apoio à sua agenda. Nós gostaríamos de aconselhar - enquanto não podemos falar como um conjunto do Anonymous – a sempre divulgar informações ao público, como nós queremos para operar em seu interesse. Quaisquer tentativas de agir em segredo, apoio às organizações políticas ou governamentais, serão desencorajados por nós ou completamente ignorado para salvaguardar nossos aliados e apoiadores que lutam pela abertura e transparência dentro dos governos, ditaduras e organizações ao redor do mundo que controlam vários aspectos de nossas vidas. Estamos do lado dos oprimidos, e não os opressores. Apoiamos as vítimas da guerra, e não a máquina de guerra. Pastebin publicado pelo membro do Anonymous AnonDiscordian, em 13 de Dezembro de 2015. Ver em http://pastebin.com/CnSdAtD1. Acesso em 20 de Maio 2016.

[103] A principal manchete foi no *Chicago Tribune* – ‘Hacker Sentenced in White House `Raid' Shrugs off His Actions’. Ver em: http://articles.chicagotribune.com/1999-11-23/news/9911230118_1_hacker-white-house-internet-electronic-assaults. Acesso em 02 de Junho de 2016.

desses ataques são influenciados por motivações políticas e essencialmente coletivas, mesmo quando são cometidos individualmente (Postmes e Brunsting, 2002).

> In sum, the Internet is changing activism profoundly. To some degree, this transformation is due to the direct influence of the Internet on collective action: opening up new avenues for it or reinforcing existing forms. However, the more fundamental change appears to be that the Internet affords movements and activists the powers of mass communication. The Internet mobilizes people by spreading alternative views and news—and the parallel emergence of subcultures supporting collective action. Indeed, the confrontational actions that are so prominent in the public eye appear to be less important in their scope and effectiveness when compared with the pervasive influence that mass communications have exerted (Postmes e Brunsting, 2002, p. 294).[104]

Essa dimensão coletiva é explícita, como nas guerras paralelas de lutas geopolíticas, mas é frequentemente implícita, por exemplo, quando as ações tais como o hacking de websites são motivados por crenças sobre a liberdade da Internet, como no caso do coletivo Anonymous. Nesse sentido, a *Operação ISIS* se perpetuou na conjuntura midiática ao ser configurada em estado traumático por "plena abordagem experimental" para alguns membros do Anonymous que designavam as ações da *#OpISIS* como "uma técnica conceitual de popularizar um movimento de hacktivismo para a mídia centralizada". Desta forma, o eixo caótico do Anonymous que determinava a luta por princípios básicos de liberdade e direitos humanos havia sido declarada subdividida pelo próprio grupo de hackers e ativistas.

---

[104] Tradução nossa: Em suma, a Internet está mudando o ativismo profundamente. Até certo ponto, esta transformação é devido à influência direta da Internet sobre a ação coletiva: a abertura de novos cenários de ações ou fortalecimento das formas existentes. No entanto, a mudança mais fundamental parece ser que a Internet proporciona movimentos de ativistas aos poderes de comunicação de massa. A Internet mobiliza pessoas para espalharem visões alternativas e notícias - e o surgimento paralelo de subculturas são suporte à ação coletiva. De fato, as ações de confronto que são tão proeminente ao ponto de vista do público parecem ser menos importante na sua abrangência e eficácia quando comparada com a influência penetrante que a comunicação de massa tem exercido.

3. INTELIGÊNCIA COLETIVA NO ANONYMOUS

O Anonymous é um movimento pluralista, em que coexistem e se complementam em diferentes pontos de vista e ideologias. Coleman (2013) concorda dizendo que a diversidade e vitalidade da ideologia política do grupo é um componente essencial da cultura do coletivo Anonymous. Esta vibração de visões políticas tem contribuído diretamente, até agora, ao sucesso e a eficácia de uma inteligência coletiva.

> Anonymous represents a participatory collective. Non-tech savvy individuals are welcome to participate in Anonymous' activities: one may, for instance, choose to help others write press releases and reports, or to give media interviews; people who have designing skills can use their abilities for designing propaganda posters or editing videos, and so on. To join the group, one simply has to identify with Anonymous and its core values. Anonymous neither expects particular abilities, nor requires them from those individuals willing to join. While 'true' hackers' opinions and skills may be respected and/or appreciated within Anonymous, they don't erect entrance barriers nor control the evolution of Anonymous (Coleman, 2013, p.12).[105]

Coleman (2013) também fornece insights sobre como os membros do Anonymous escolhem seus alvos. A pesquisadora propõe que as operações do coletivo são reativas, e que vários eventos ou incidentes locais e internacionais podem servir como impulso para as ações do Anonymous. O grupo representa a coexistência de diversidades de indivíduos da comunidade virtual que reagem a eventos ao invés de escolhê-los aleatoriamente ou de maneira caótica.

Portanto, a questão é que o Anonymous se origina de uma inteligência distribuída que faz uso do conhecimento coletivo (Coleman, 2012). O argumento aqui

[105] Tradução nossa: O Anonymous representa um coletiv participativo. Indivíduos não tão experientes em tecnologia são bem-vindos a participar das atividades do Anonymous: pode-se, por exemplo, optar por ajudar os outros a elaborar comunicados de imprensa e relatórios, ou para conceder entrevistas para a mídia; pessoas que têm habilidades de design podem usar suas habilidades para a concepção de cartazes de propaganda ou edição de vídeos, e assim por diante. Para se juntar ao grupo, um simplesmente tem de se identificar como Anonymous e seus valores fundamentais. Anonymous não necessita de habilidades particulares, nem é exigido daqueles indivíduos dispostos a participar. Enquanto as opiniões e habilidades dos "verdadeiros" hackers "podem ser respeitados e/ou apreciados dentro do Anonymous, eles não se responsabilizam pela emancipação, nem controlam a própria evolução do Anonymous.

proposto é que, por um lado, o grupo Anonymous se configura em um aspecto distribuído em rede de inteligência. Por outro lado, existem núcleos de conhecimento e ação nesta rede que apresentam assimetrias de poder imanentes na sociedade da informacão ao permitir às organizações poderosas, como as instituições de estado - neste caso para o Anonymous, o FBI - para monitorar e tentar controlar estruturas em rede (Levy, 2015).

> O ciberespaço com suporte de inteligencia coletiva é uma das principais condições de seu próprio desenvolvimento. Toda a história da cibercultura testemunha largamente sobre esse processo de retroação, ou seja, sobre a auto manutenção da revolução das redes digitais. Em primeiro lugar, o crescimento do ciberespaço não determina automaticamente o desenvolvimento da inteligência coletiva, apenas fornece a esta inteligência um ambiente propício (Levy, 2014, p.29-30).

Hakim Bey (2011), ao configurar a TAZ[106] nas comunidades virtuais, estabelece a ligacão entre a cultura hacker e o aperfeiçoamento do computador pessoal na década de 1960, como um passo revolucionário cotidiano e independente, que visa à liberdade individual de atores que contribuem para a resistência da Internet na Era da Informação, apresentando os hackers como personagens influentes na libertação autónoma da consciência coletiva na Internet.

Durante a propagação de grupos ligados ao Anonymous decorrentes das ações da Operação HBGary, Operação PayBack, Operação Primavera Árabe, Operação Israel e Operação BART, ramificações como LulSec e AnonOps se perpetuaram no eixo da ideia do Anonymous que eventualmente, a partir de 2013, se eternizou com o estigma do hacktivismo contemporâneo com capacidade de operar sem uma liderança e a difusão de ideias libertárias que buscam influenciar a comunidade virtual. A concepcão da inteligência coletiva do Anonymous é assim "operada por meio da interatividade

[106] Zona Autônoma Temporária, p.34, 2011. O que chamamos de TAZ desenvolve-se como um levante, algo excepcional na história , que, apesar de muitos classificarem como uma revolução que fracassou, eleva o grau de intensidade da vida e da consciência, cujos exemplos não passaram de pura simulação, acabando com uma opressão e estabelecendo outra- são desmistificadas no livro, incitando a formação de um novo tipo de revolucionar cotidiano e independente. Visar à liberdade de todos serviu, por muitas vezes, como máscara de interesses particulares e opressores. Os princípios da TAZ são: liberdade independente e autônoma. Por tais características, a TAZ se assemelha muito ao comunalismo intencional e ao comunalismo libertário, chamados por Kenneth Rexroth, simplesmente, de comunalismo.

entre indivíduos diversificados entre si, que vivenciam uma linha histórica da tecnologia conectada à sociedade da informação que fornecem meios alternativos de uma subcultura das entranhas da Internet na década de 80" (Castells, 2013, p. 47).

3.2 A NOVA FASE DO HACKTIVISMO

Para Castells (2003), só a capacidade de criar tecnologia e de compartilhá-la com a comunidade são valores respeitados. Para os hackers, a liberdade é um valor fundamental, particularmente a liberdade de acesso à sua tecnologia e a de usá-la como bem entendem. Esse valor é indispensável à dinamica cultural de múltiplas camadas gerada pelo mundo da Internet, inclusive em especial, de um ambiente inóspito criado pelos hackers do Anonymous para propagar conhecimento didático e técnicas de hacking direcionadas aos usuários da Internet: o canal OnionIRC.

Figura 17: Símbolo do canal OnionIRC

Este novo método de apropriação da capacidade de interconexão é influenciada pela formação de comunidades online que reiventaram a sociedade e, nesse processo, expandiram espetacularmente a interconexão de computadores e a acessibilidade entre os usuários (Castells, 2003). O navedor de anonimato Tor elucida esse cenário ao atrair a comunidade hacker que recentemente vem adotando valores tecnológicos da meritocracia ao defender a crença dos hackers no valor da liberdade, da comunicação

horizontal e da interconexão interativa[107], ao utilizar o canal como uma ferramenta de resistência contra modelos tradicionais de comunicação ativa, na prática da tecnologia pela tecnologia[108].

O OnionIRC foi estabelecido em Abril de 2016, gerenciado por dois membros da comunidade do Anonymous: *butts* e AnonDiscordian. O método de acesso foi divulgado em massa pelo perfil oficial do Twitter, o @OnionIRC, ao publicar um guia básico[109] para se conectar à rede Tor e acessar o canal.

> I always wanted a project where everyone would be Anonymous and torified IRC network was the best way to accomplish this. And butts wanted an old teaching project formely known as Black Hat Academy back. So I approached him and he created OnionIRC.[110]

A intenção do projeto é oferecer aos usuários entusiastas uma maneira de navegar e compartilhar informações de maneira anônima e ainda ter a oportunidade de aprender métodos e tecnicas de cibersegurança para proteção pessoal contra sistemas de vigilância da Internet. A partir deste ponto, é importante ressaltar a cultura da Internet é uma cultura formada por uma crença tecnocrática no progresso dos indivídus através da tecnologia, levando a cabo por comunidades de hackers que prosperam na criatividade tecnológica livre e aberta, inserida em redes virtuais que pretendem reiventar a sociedade (Castells, 2003).

Nesta lógica, a comunidade do Anonymous é vista recentemente como um núcleo fragmentado de uma subdivisão da cultura hacker, embora seja uma subcultura construída sobre princípios políticos, bem como sobre resistencia e revolta pessoal. Para Richard Stallman, todo o processo de busca por meios alternativos de evasão tecnológica pelos grupos de hackers é um componente essencial da liberdade de expressão na Era da Informação. Assim como a Fundação do Software Livre de

---

[107] Castells, 54.

[108] Castells, 53.

[109] Guia de acesso para o OnionIRC, em portugues: https://ghostbin.com/paste/3ofay. Acesso em 30 de Maio 2016.

[110] Tradução nossa: Eu sempre quis um projeto onde todos seriam Anonymous e uma rede estruturada pelo Tor foi a melhor maneira de conseguir isso. E butts queria uma antigo projeto didático conhecido como Black Hat Academy de volta. Então fiz a proposta à ele e assim criou o OnionIRC. AnonDiscordian em resposta durante entrevista, em 09 de Maio de 2016.

Stallman, o OnionIRC dedica-se a proteger os usuários mobilizando-os a compreender técnicas e ferramentas de hacking para que se una esforços por manter sua criação coletiva fora do alcance de governos e corporações.

> Mas o que é comum à cultura hacker, em todos os contextos sociais, é a premência de reiventar maneiras de se comunicar com computadores e por meio deles, contruindo um sitema simbiótico de pessoas e computadores em interação na Internet A cultura hacker é, em essência, uma cultura de convergência entre seres humanos e suas máquinas num processo de interação liberta. É uma cultura de criatividade intelectual fundada na liberdade, na cooperação, na reciprocidade e na informalidade (Castells, 2003, p. 45).

Ao serem questionados sobre o desempenho e a utilidade da rede de anonimato OnionIRC, usuários do canal principal aprovaram a iniciativa em ter acesso a uma rede de chat instantâneo sem a necessidade de identificação verdadeira. “Me juntei ao canal por estar interessado em hacktivismo e as demais técnicas de hacking”, disse o usuário anônimo Gruben. “Tenho certeza que aqui é o lugar certo para quem quer este tipo de conhecimento de graça”, concluiu. Na prática, uma minoria declara que se juntou à comnunidade do OnionIRC pela nostalgia dos momentos em que o coletivo Anonymous era reconhecido pelo canal de IRC AnonOps, durante a era do grupo LulzSec, em 2011, e pela sensação de ter a chance de trazer aos usuários novatos alguns princípios básicos da antiga escola de hackers online Blackhat Academy[111].

> Blackhat Academy was very successful, but simply died over time due to staff moving on to other projects. Another previous school ran by some of the same people predating Blackhat Academy was called School4Lulz. One main difference here is that we are encouraging the community members to get involved and give classes rather than expecting the staff to do them all. Blackhat Academy also did not take advantage of anything like the Tor network, so it was often under DDoS attacks and the cost of running the network became too much at times.[112]

[111] O Blackhat Academy foi um projeto de escola virtual com o objetivo de treinar hackers e entusiastas base técnicas de ciberseguranca e protecao contra hackers, operado entre 2011 e 2012.

[112] Tradução nossa: Blackhat Academy foi bem sucedida, mas simplesmente parou ao longo do tempo devido à dedicacacão da equipe em outros projetos. Outra antiga escola conduzida por algumas das mesmas pessoas do Blackhat Academy foi chamada de School4Lulz. A principal diferenca aqui é que estamos incentivando os membros da comunidade a se envolver e dar aulas ao invés de esperar a equipe

Durante uma conversa no chat OnionIRC, outro usuário esclareceu a questão de que o hacktivismo irá prosperar se iniciativas como o OnionIRC surgirem com mais frequência. “O que me motiva: espalhar conhecimento e continuar com o legado do que me foi ensinado sobre todas as coisas que eu já sei. Acredito que o hacktivismo irá se tornar mais crítico em um futuro próximo”, disse rackham.

para fazer. Blackhat Academy também não tira proveito de nada como a rede Tor, por isso esteve muitas vezes sob ataques de DDoS e os custos de funcionamento da rede não eram o bastante. O responsável pela iniciativa OnionIRC *butts*, ao conceder entrevista, em 09 de Maio de 2016.

CONSIDERAÇÕES FINAIS

Em razão do hacktivismo do coletivo Anonymous inserido como uma contracultura de resistência, o mundo metafísico da informação no ciberespaço se manifesta no mundo dos hackers como uma irreverência às políticas e tecnologias destinadas a limitar o fluxo de informações (Kelly, 2004). Visto assim, Coleman (2012) afirma que o grupo Anonymous é ainda reconhecido essencialmente pela atitude de que a "informação quer ser livre", como seu direito para libertar a informaçao de forças opressivas como esquemas de proteção de direitos autorais, leis de propriedade intelectual, sistemas de vigilância global e atravessar firewalls de rede corporativos.

A conclusão normativa determinada sobre os hackers do Anonymous é que apesar de sua moralidade tradicional, é possível concluir que além da diversidade de suas ações políticas e operações coletivamente orquestradas, o Anonymous desenvolve a partir de suas habilidades específicas e experiências de vida, novos modos para colaborar, organizar e protestar (Coleman, 2011). Na maioria dos casos, como nas operacões Projeto Chanology (2008), HBGary (2010), PayBack (2011), BART (2010), Primavéra Árabe (2013) e entre outras, o Anonymous catalisou debates sobre seus ataques de negação de serviço distribuídos ou DDoS, como forma de protesto legítimo e ainda propiciou um alarde formidável para a imprensa internacional.

> Digital media have certainly played a crucial role in establishing mechanisms for communication, shifting social relationships, and cultivating collective political interests, but in less tectonic ways than often assumed by the term digital generation. Instead of sweeping conceptual categories that brush over the enormous plurality of digital experience, it pays to use terminology and frameworks that capture with more nuance different forms of experience, including different degrees and types of technological saturation (Coleman, 2011, p. 512).[113]

[113] Traducão nossa: Os meios digitais têm certamente desempenhado um papel crucial no estabelecimento de mecanismos para a comunicação, mudando as relações sociais, e cultivando interesses políticos coletivos, mas de maneiras menos tectônicas do que muitas vezes assumidas pela geração digital. Em vez de categorias amplas conceituais que articulam sobre a enorme pluralidade de experiência digital, vale a pena usar a terminologia e estruturas que capturam com diferentes formas de experiência, incluindo os diferentes graus e os tipos de saturação tecnológica.

Dada a trajetória do Anonymous como parte ascensão da Internet da década de 90, o coletivo reconhece e executa uma sensibilidade em torno das particularidades da ética hacker. Se o Anonymous aparece como uma máquina de guerra, é porque foi corrompido, desmantelado e impelido durante processo de reconstruir sua imagem para a comunidade virtual (Coleman, 2011). Visto assim, os Anons apresentam uma sofisticação afetiva quando se trata de sucessos susceptíveis a fracassos.

O coletivo em questão é, no entanto, uma insurgência gerada pelos princípios caóticos que a Internet das entranhas do MIT durante a década de 60 trouxe à comunidade virtual do século XXI a perspectiva de idolatria tecnológica propagada por Richard Stallman, Steve Wozniak[114], Steve Jobs, Linus Torvalds[115] para ícones da luta pela liberdade de informacão na Internet nos dias de hoje como Aaron Swartz[116], Jeremy Hammond[117], Barret Brown, Julian Assange, Chelsea Manning[118], Edward Snowden e Lauri Love[119].

[114] Wozniak fundou a Apple com Steve Jobs e Ronald Wayne, em 1976. Mas Wozniak era o único que projetou e construiu o primeiro produto da gigante de tecnologia, o Apple 1. Steve terminou seu curso de graduação na Universidade da Califórnia, Berkeley. Ver em http://www.cnbc.com/2016/04/21/steve-wozniak-school-is-not-enough-go-beyond-it.html. Acesso: 28 de Maio 2016.

[115] Desenvolvedor do Linux, um sistema operacional de código aberto que pertence à plataforma UNIX de sistemas operacionais.

[116] Foi um programador estadunidense e ativista na Internet. Swartz foi co-autor da criação do RSS. Foi um dos fundadores do Reddit e da organização ativista online *Demand Progress*. Swartz era contrário à prática da revista científica *JSTOR* por remunerar editoras e não remunerar os autores e cobrar o acesso aos artigos, limitando o acesso para comunidades acadêmicas. Dois anos depois, na manhã do dia 11 de janeiro de 2013, Aaron foi encontrado enforcado no seu apartamento em Crown Heights, Brooklyn - num aparente suicídio. Após a sua morte, a promotoria federal de Boston retirou as acusações contra ele. Ver em: https://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy. Acesso: 28 de Maio 2016.

[117] Jeremy é um hacktivista político de Chicago, condenado e sentenciado em Novembro de 2013 a 10 anos na prisão federal dos EUA por ter hackeado a empresa privada de inteligência Stratfor e liberado os documentos para o WikiLeaks.

[118] Nascida sob o sexo masculino e de nome Bradley Edward Manning (Crescent, 17 de dezembro de 1987), é uma militar transexual do Exército dos Estados Unidos que foi presa e processada por acesso e divulgação de informações sigilosas que resultaram no escândalo conhecido como "Cablegate" , referindo-se aos telegramas diplomáticos americanos que começaram a ser publicados em novembro de 2010 pelo Wikileaks e cinco grandes jornais. Sua detenção foi realizada em maio de 2010, enquanto servia às tropas norte-americanas no Iraque. Ver em: https://www.theguardian.com/us-news/2016/may/27/chelsea-manning-six-years-prison-whistleblowing. Acesso: 28 de Maio 2016.

[119] Lauri Alexander Love é um hacker britânico acusado de roubar dados de computadores do Governo dos Estados Unidos, incluindo a Reserva Federal, o Exército dos EUA, Agência de Defesa de Mísseis, e a NASA apenas utilizando habilidades básicas de hacking. Ver em: http://s.telegraph.co.uk/graphics/projects/hacker-lauri-love-extradition/. Acesso: 28 de Maio 2016.

REFERÊNCIAS

ASSANGE, Julian. **Cypherpunks**: Liberdade e Futuro da Internet. Editora: Boitempo Editorial. Porto Alegre, 2013.

BEY, Hakim. **TAZ:** Zona Autônoma Temporária. 03 ed. São Paulo: Conrad Editora, 2011.

CASTELLS, Manuel. A Galáxia da Internet. Rio de Janeiro: Editora Zahar, 2003.

COLEMAN, Gabriella. **Beacons of Freedom:** The Changing Face of Anonymous. London: Index on Censorship, 2012.

COLEMAN, Gabriella. **Coding Freedom:** The Ethics and Aesthetics of Hacking. Princeton University Press, 2012.

COLEMAN, Gabriella. **Hacker, Hoaxer, Whistleblower, Spy**: The many faces of Anonymous. London: Ed. Verso, 2014.

COLEMAN, Gabriella. Hacker Politics and Publics. Public Culture. Duke University Press, 2011. Vol. 23.

COLEMAN, Gabriella. **Our Weirdness Is Free:** Online army, agent of chaos, and seeker of justice. New York: The 15th Triple Canopy, 2012.

GALLOWAY, Alexander. Protocol. The MIT Press. Massachusetts, 2004.

GRAMMATIKOPOULOU, Christina. **From the Deep Web to the City Streets:** Hacking, Politics and Visual Culture. Universitat de Barcelona: antropologia.cat, 2013, n.19.

HIMANEM, Pekka. The Hacker Ethic and the spirit of the information age. New York: Random House Trade Paperbacks, 2001.

JORDAN, Tim; TAYLOR, Paul. A Sociology of hackers. The Editorial Board of the Sociological Review. Oxford: Blackwell Publishers, 1998.

LEMOS, André. **Cibercultura:** tecnologia e vida social na cultura contemporânea. 06 Ed. Porto Alegre: Editora Sulina, 2013.

LÉVY, Pierre. **A inteligência coletiva:** Por uma antropologia do ciberespaço. Ed. 10. São Paulo: Edições Loyola, 2015.

LÉVY, Pierre. Cibercultura. Editora 34, Rio de Janeiro: Fundação Biblioteca Nacional, 1999.

LEVY, Steven. Os Heróis da Revolução. São Paulo: Editora Évora, 2012.

KELLY, Liam. **Hacking Systems, Hacking Values:** Interactive Theories for an Interactive World. Dep. Of Science and Technology Studies, Virginia Polytechnic Institute and State University, 2004.

MACHADO, Murilo Bansi. **Anonymous Brasil:** Poder e Resistência na Sociedade de Controle. Salvador: EDUFBA, 2013.

MCLAUGHLIN, Victoria. **Anonymous:** What do we have to fear from hacktivism, the lulz, and the hive mind? Program in Political and Social Thought at University of Virginia, 2012.

OLSON, Parmy. Nós Somos Anonymous. São Paulo: Editora Novo Século, 2014.

POSTMES, Tom; BRUNSTING, Suzanne. Collective Action in the Age of the Internet. Social Science Computer Review, 20: 290-301. University of Amsterdam, 2012.

SAMUEL, Alexandra. Hacktivism and the Future of Political Participation. Harvard University. Massachusetts, 2004.

SAUTER, Molly. Distributed Denial of Service Actions and the challenge of civil disobedience on the Internet. MIT Media Lab. Massachusetts, 2013.

SILVEIRA, Sérgio Amadeu. Ciberativismo, cultura hacker e o individualismo colaborativo. São Paulo: Revista USP - n. 86, p. 28-39, 2010.

UGARTE, David. O poder das redes. Porto Alegre: EdiPUCRS, 2008.